jamk

AWS Lokilähteet

Henry Muhonen

Opinnäytetyö, AMK
Toukokuu 2023
Tietojenkäsittely ja tietoliikenne
Insinööri (AMK), Tieto- ja viestintätekniikka

jamk | Jyväskylän ammattikorkeakoulu
University of Applied Sciences

jamk

Kuvailulehti

Muhonen, Henry

AWS Lokilähteet

Jyväskylä: Jyväskylän ammattikorkeakoulu. Toukokuu 2023, 28 sivua

Tietojenkäsittely ja tietoliikenne. Tieto- ja viestintätekniikan tutkinto-ohjelma. Opinnäytetyö AMK.

Julkaisun kieli: suomi

Julkaisulupa avoimessa verkossa: kyllä

Tiivistelmä

Erilaisten pilvipalvelujen kasvu on johtanut siihen, että yhä useampi yritys on ottanut käyttöön pilvipohjaisia palveluita oman liiketoimintansa järjestämiseen ja ylläpitämiseen. Palvelut siirtyvät pois yritysten omista konesaleista sekä omilta servereiltä ja siirretään pilveen pilven skaalautuvuuden sekä edullisuuden vuoksi. Näin ollen niistä saatavat lokilähteet voivat muuttua ja täten ymmärrys sekä osaaminen mitä lokilähteitä pilvipalvelusta on saatavilla kasvaa.

Tavoitteena opinnäytetyössä on tutustua Amazon Web Services (AWS) pilviympäristön erilaisiin palveluihin ja niiden lokilähteisiin, jotta tarpeelliset lokilähteet saadaan jalostettua esimerkiksi turvallisuusoperaatiokeskuksien (Security Operations Center (SOC)) tarpeisiin.

Tutkimus tehdään AWS ympäristöön tutustumalla ja tutkimalla lokilähteitä, miten ne saadaan käyttöön sekä mitä asetuksia lokilähteille annetaan, jotta tarvittava tieto on saatavilla tilanteen tarkempaa tutkimista varten. Lokilähteiden lisäksi on tarkoitus tutkia millä tavalla loki on luettavissa AWS ympäristön natiiveilla sovelluksilla.

Lopputuloksena lisättiin ymmärrystä AWS-ympäristön lokilähteistä, niiden asetuksista sekä lokilähteiden tutkimisesta pilvipalveluympäristössä.

Avainsanat (asiasanat)

AWS, Lokilähteet, Pilvipalvelu, SOC

Muut tiedot (salassa pidettävät liitteet)

jamk

Description

Muhonen, Henry

AWS log sources

Jyväskylä: JAMK University of Applied Sciences, May 2023, 28 pages

Engineering and technology. Degree Programme in Information and Communication Technology. Bachelor's thesis.

Permission for open access publication: Yes

Language of publication: Finnish

Abstract

The growth of various cloud services has led to the fact that more and more companies have adopted cloud-based services to organize and maintain their business. The services are moved away from companies own datacenters and servers and are moved to the cloud due cloud services giving more room with scalability and affordability. Consequently the log sources obtained from cloud services changes and thus the understanding and knowledge of which log sources are available from the cloud increases.

The aim of the thesis is to become familiar with the various services of Amazon Web Services (AWS) cloud environment and which log sources are available so necessary log sources can be refined for needs of, for example, Security Operation Center (SOC).

The research is done by familiarizing with the AWS environment and examining the log sources, how they can be used and what settings needs to be activated to the log sources, so that the necessary information is available for more detailed investigation. Addition to log sources, plan is also to investigate how the log could be read by native applications in the AWS environment.

The end result increased understanding of log sources in the AWS environment, their settings and how the investigation happens in cloud computing environment.

Keywords/tags (subjects)

AWS, Log sources, Cloud Computing, SOC

Miscellaneous (Confidential information)

Sisältö

Kuviot

Taulukot

No table of figures entries found.

1 Johdanto ja toimeksiantaja

Erilaisten pilvipalvelujen kasvu on johtanut siihen, että yhä useampi yritys on ottanut käyttöön pilvipohjaisia palveluita oman liiketoimintansa järjestämiseen ja ylläpitämiseen. Palvelut siirtyvät pois yritysten omista konesaleista sekä omilta servereiltä ja siirretään pilveen pilven skaalautuvuuden sekä edullisuuden vuoksi. Näin ollen niistä saatavat lokilähteet voivat muuttua ja täten ymmärrys sekä osaaminen erilaisista lokilähteistä pilvipalvelussa kasvaa.

Tavoitteena opinnäytetyössä on tutustua Amazon Web Services (AWS) pilviympäristön erilaisiin palveluihin ja niiden lokilähteisiin, jotta tarpeelliset lokilähteet saadaan jalostettua turvallisuusoperaatiokeskuksien (Security Operations Center (SOC)) tarpeisiin. AWS-ympäristöstä tuleva loki sekä lokeista koostuvat hälytykset tarvitsevat ymmärrystä sekä mahdollisia ohjeita, kuinka näitä tapahtumia saadaan tutkittua paremmin ja näin tuoda arvoa sekä SOC:ille ja sen asiakkaille. Tälläinen SOC löytyy opinnäytetyön toimeksiantajalta Elisa Santa Monica Oy:lta.

Elisa Santa Monica Oy on Elisa Oyj:n tytäryhtiö, jonka Elisa Oyj osti vuonna 2017. Elisa Santa Monica on vuonna 2004 perustettu yritys, joka ennen Elisa Oyj:hin liittämistä kulki nimellä Santa Monica Networks. Elisa Santa Monica Oy:lla työskentelee 170 henkilöä ja sen liikevaihto on noin 63 miljoonaa euroa (Elisa Santa Monica taloustiedot n.d.). Elisa Santa Monica tuottaa asiantuntija palveluita ja nämä palvelut voidaan jakaa neljään ryhmään: tietoverkot, datakeskukset, tietoturva sekä koulutuspalvelut (Elisa Santa Monica n.d.).

Tutkimus tehdään tutustumalla AWS-ympäristöön, sen palveluihin sekä näistä saataviin lokilähteisiin, miten ne saadaan käyttöön sekä mitä asetuksia lokilähteille annetaan, jotta tarvittava tieto on saatavilla tilanteen tarkempaa tutkimista varten. Pääpainona identiteetti- sekä käyttöoikeushallinnasta saatavat lokilähteet, käyttöjärjestelmä sekä sovelluslokit sekä Amazonin pilvessä tapahtuvat internet tapahtumat. Lokilähteiden lisäksi on tarkoitus tutkia millä tavalla loki on luettavissa AWS-ympäristön natiiveilla sovelluksilla.

2 Teoriatausta

2.1 Loki

Loki on tallenne organisaation järjestelmissä ja verkoissa tapahtuvista tapahtumista. Lokit koostuvat lokimerkinnöistä ja jokainen merkintä sisältää tietoa liittyen tiettyyn tapahtumaan, joka tapahtui ympäristössä tai verkossa. Tietoturvalokien määrä, volyymi sekä moninaisuus ovat lisääntyneet huomattavasti mikä on luonut tarpeen hallinnoida prosessia, jolla lokia tallennetaan, luodaan, lähetetään, analysoidaan sekä hävitetään. (Kent & Souppaya 2006.) Lokia tuottaa melkein jokainen verkon laite ja lokia käytetään niin ympäristön ongelmien selvittämiseen, virhetilanteiden tutkintaan, haitallisen toiminnan havainnoimiseen kuin järjestelmien sekä verkkojen optimoimiseen. (Todd 2017.)

2.1.1 Lokityypit

Laite- ja verkkoinfrastruktuurin lokit voidaan karkeasti jakaa kolmeen eri pääryhmään: infrastruktuurin laitteisto-, palvelu- ja sovelluslokeihin. Laitteisto lokit ovat laitteiston toimintaan liittyviä tapahtumia. Lokien lähteet voivat olla reitittimen tai kytkinten tapahtumia ja näillä lokeilla voidaan seurata reitittimien tai kytkinten liikennettä, tarkistella ongelmia sekä havaita epänormaali toiminta. Palvelulokilähteitä voivat olla laitteistojen päälle rakennettujen palveluiden kuten DHCP:n (Dynamic Host Configuration Protocol) antamat IP-osoite lokit. Hyvin konfiguroidussa ympäristössä voidaan seurata koko ajan mikä laite on minkäkin IP osoitteen takana ja näin korreloida tapahtumia muiden lokien kanssa, jotka eivät välttämättä näe tai saa muita laitteen tietoja. Sovelluslokit seuraavat sovelluksiin tehtäviä muutoksia ja on tärkeää tietää kuka sovellusta on käyttänyt, mitä sovelluksella on tehty ja mitä komentoja sovellukseen on syötetty. (Todd 2017.)

2.1.2 Lokin sisältö

Laitteet ja sovellukset voivat antaa lokit monessa eri muodossa. Tutuin ja helppokäyttöisin muoto lokille on tekstimuotoiset lokit, joita ihminen pystyy lukemaan. Vaikka lokilähde antaisikin tekstimuotoista lokia, ei se välttämättä ole helposti ymmärrettävää. Loki voi olla tekstin pätkä, joka kertoo hyvin perus asiat tapahtumasta. Todd (2017) mukaan lokissa pitäisi olla mukana ainakin seuraavat tietokentät: päivä, aika, aikavyöhyke, mistä lokilähteestä loki on, tapahtuman severiteetti sekä tieto siitä mitä on tapahtunut. Nämä tietokentät antavat hyvän perustiedon mitä ja milloin on

tapahtunut. Aikavyöhyke on tärkeä tietokenttä, jos lokia siirretään esimerkiksi analysoitavaksi eteenpäin sillä aikavyöhykkeet voivat muuttua, joka johtaa siihen, että lokin tutkinta voi vaikeutua. Riippuen lokilähteestä tietokenttiä voi olla muitakin, esimerkiksi sovellus voi tarjota sovellukseen tehtävät komennot lisänä edellisiin tietokenttiin tai vanhoihin tietokenttiin voidaan korreloida lisää tietoa muista lokilähteistä. Tekstimuotoinen loki, ainakin jos sitä joudutaan tallentamaan pitkiä aikoja, voi viedä paljonkin tallennustilaa. Loki voi olla myös binäärimuotoista, jolloin sen tutkiminen sekä ymmärtäminen voi olla ihmiselle ongelmallista. Näin ollen binäärimuotoinen loki vaatii tavan lukea kyseistä lokia. Tämä onkin binäärimuotoisen lokin huomattavin ongelma, vaikka on tekstimuotoiseen lokiin verrattaen kompaktimpi, vie vähemmän kaistaa siirrettäessä sekä vähemmän prosessointi tehoa laitteilta (Todd 2017).

2.2 Pilvipalvelut

Erilaisten pilvipalvelujen kasvu on johtanut siihen, että yhä useampi yritys on ottanut käyttöön pilvipohjaisia palveluita oman liiketoimintansa järjestämiseen ja ylläpitämiseen. Pilvipalvelut ovat hyvin skaalautuvia moniin eri tehtäviin ja niihin on helppo avata uusia palveluja. Ne ovat yleisesti myös edullinen vaihtoehto, sillä monet maailmanlaajuiset yritykset kuten Microsoft, Google sekä Amazon ovat investoineet sekä kehittäneet laajoja pilvipalveluratkaisuja asiakkailleen.

Pilvipalvelut tarkoittavat yleisesti verkkopalvelua, joka mahdollistaa tiedon tallentamisen ja käyttämisen etäpalvelimilla. Sen sijaan että yritys tai yksityishenkilö ostaisi ja ylläpitäisi fyysisiä datakeskuksia tai palvelimia, voidaan käyttää palvelun tarjoajien palveluja kuten tallennustilaa, laskentatehoa tai tietokantapalveluja. (Microsoft Azure n.d.) National institute of standards and technology julkaisu (Mell & Grance 2011) selittää pilvipalvelun mallina, joka mahdollistaa internetin yli heti saatavilla olevan joukon palveluja esimerkiksi verkon, tallennustilan, laskentatehon sekä sovellukset, jotka voidaan pystyttää nopeasti ja pienellä vaivalla.

Pilvipalvelut voidaan lajitella National Institute of Standards and Technolgy julkaisun (Mell & Grance 2011) mukaan kolmeen erilaiseen palvelumalliin, IaaS (Infrastructure as a service) eli infrastrucktuuri palveluna, PaaS (platform as a service) eli alusta palveluna sekä SaaS (software as a service) eli ohjelmisto palveluna. Mell ja Grance (2011) selittävät SaaS palvelun siten, että palvelun tarjoajalla on sovellus, joka pyörii pilvipalvelun päällä. Sovellus on käytettävissä erilaisista laitteista kuten verkkoselaimesta tai muusta ohjelman käyttöliittymästä. Palvelun käyttäjä ei hallitse tai

valvo taustalla olevaa pilvi-infrastruktuuria esimerkiksi verkotusta, palvelimia, käyttöjärjestelmää tai tallennustilaa eikä välttämättä edes kaikkia sovelluksen ominaisuuksia.

PaaS eroaa SaaS:in palvelumallista tarjoamalla alustan omien sovellusten kehittämiseen, testaamiseen ja käyttöönottoon (Mell & Grance 2011). Näin käyttäjä voi luoda omanlaisen sovelluksen pilviympäristöön ja samoin kuin SaaS mallissa käyttäjän ei tarvitse hallita tai valvoa pilvi-infrastruktuuria. Kuitenkin PaaS mallissa käyttäjällä on pilviympäristössä olevan sovelluksen kaikki oikeudet. IaaS palvelumalli tuo käyttäjälle vielä enemmän valtaa pilviympäristön konfiguroimiseen. Tässä mallissa pilvipalvelun tarjoaja tarjoaa käyttäjälle virtuaalisen infrastruktuurin aina virtuaalipalvelimista verkon konfigurointiin sekä tallennustiloihin. Käyttäjällä on vapaimmat kädet luoda ja tehdä muutoksia pilviympäristöön verrattuna edellä mainittuihin malleihin. Alla olevassa taulukossa 1 näkyvät eri pilvipalvelumallien vastuunjako aina sovelluksesta verkkolaitteisiin. Siitä myös nähdään että itse ylläpidettävässä palvelussa joudutaan itse hoitamaan koko ympäristöä, kun taas PaaS mallissa itse joudutaan ylläpitämään vain sovellusta ja tietoa, jonka sovellus tarvitsee tai tallentaa.

Taulukko 1. Pilvipalvelumallien vastuunjako (Amazon what is IaaS, N.d). Muokattu.

Vihreä: omalla vastuulla Keltainen: Pilvipalvelun tarjoajan vastuulla	Eri pilvipalvelumallien vastuunjako			
	Paikallinen ympäristö (“on-prem”)	Infrastruktuuri palveluna	Alusta palveluna	Ohjelmisto palveluna
Sovellus				
Tiedot				
Ohjelmisto, jolla sovellusta ylläpidetään				
Ohjelmisto, jolla monitoroidaan sovellusta				
Käyttöjärjestelmä, jolla sovellusta käytetään				
Virtualisointi teknologia				
Palvelinkoneet				
Tallennustila palvelimet				
Verkkolaitteet				

2.3 Amazon Web Services

Amazon Web Services (AWS) on maailman kattavin ja laajimmin hyväksytty pilvipalvelualusta, joka tarjoaa yli 200 täysin varusteltua palvelua datakeskuksista maailmanlaajuisesti. AWS on myös suunniteltu olemaan joustavin ja turvallisin pilvipalvelu ympäristö ja sen ydininfrastruktuuri on rakennettu täyttämään esimerkiksi armeijan, pankkien ja muiden mahdollisesti arkaluontoisten organisaatioiden tietoturvallisuus vaatimukset. AWS-ympäristö hyödyntää uusinta teknologiaa, jotta käyttäjät voivat kokeilla ja innovoida ympäristössä mahdollisimman vapaasti. AWS myös kehittää itseään jatkuvasti tuottaakseen uusia teknologioita, jotka helpottavat käyttäjiä sekä yrityksiä. (Amazon AWS n.d.) AWS itsessään on PaaS mallin mukainen ympäristö, jonka sisälle on rakennettu niin SaaS palveluita, esimerkiksi Amazon WorkMail, kuin IaaS palveluita, kuten Amazon EC2.

2.3.1 AWS lokilähteet

AWS-ympäristön palvelut ovat tehty helpottamaan pilvipalvelujen käyttämistä. Pilvipalvelut tarjoavat erilaisia palveluita riippuen käyttäjän tarpeista ja palvelut ovat hyvin joustavia. Koska työn aiheena on AWS-ympäristön lokilähteet, syvennymme tarkemmin palveluihin, joista saatavat lokilähteet ovat mielenkiintoisia ja tarpeellisia työn kannalta.

AWS:ssa on valittavana alueita (region), mille luoda oma ympäristö. Alue valitaan ympäristön tarpeiden mukaan, joita voivat olla geolokaatio käyttäjän ja valitun alueen välillä, geolokaatio tiedon tallentamisen osalta tai jopa GDPR (General Data Protection Regulation) mukaiset tietosuoja asetukset. AWS alueet saadaan keskustelemaan keskenään, mutta alueen valinta ympäristöä pystyttäessä sekä alueen valinta eri palveluille on syytä ottaa huomioon.

2.3.2 AWS IAM

AWS Identity and Access Management (IAM) eli identiteetti- ja käyttöoikeushallinta palvelua käytetään käyttäjä sekä käyttöoikeus hallintaan. IAM:illa voidaan määrittää esimerkiksi käyttäjä tai resurssi mikä saa käyttää AWS-ympäristön resursseja ja palveluja (AWS IAM n.d.). Tämä tapahtuu IAM:iin tehtyjen politiikkojen sekä roolien kautta, joita AWS-ympäristöön on luotu valmiiksi, tai näitä voi luoda itse. Politiikat ovat JSON (JavaScript Object Notation) mallisia tiedostoja, joita voidaan luoda erilaisiin tilanteisiin. Kaikki oikeudet ympäristössä pohjautuvat näihin politiikkoihin ja näitä politiikkoja voidaan lisätä rooleihin tai suoraan käyttäjille. Roolit voivat olla monen politiikan

kokoelmia, jolla saadaan käyttäjille keskitetysti käyttöoikeuksia tiettyihin AWS-ympäristön palveluihin. IAM tuottaa paljon tärkeitä lokilähteitä palvelun ylläpitonäkökulmasta. Palvelusta saatavat lokilähteet ovat esimerkiksi käyttäjien kirjautumisista sekä käyttäjiin ja instansseihin tapahtuvista muutoksista tallentuvat lokitiedot. Erilaisia kirjautumismenetelmiä AWS- ympäristöön ovat perinteinen käyttäjänimi sekä salasana, API (Application Programming Interface) avain, jolla saadaan yhteys AWS-ympäristöön esimerkiksi komentoriviltä sekä Security Token Service (STS) tunnisteella, joka on väliaikaisesti luotu tunnus käyttäjälle. STS vaatii kirjautumisen ympäristöön käyttäjänimellä sekä salasanalla tai API avaimella.

2.3.3 Amazon S3

Amazon Simple Storage Service (S3) tai Amazon S3 on tallennuspalvelu, joka tarjoaa alan johtavaa skaalautuvuutta, tiedon saatavuutta, turvallisuutta ja suorituskykyä (AWS S3 2023 n.d.). Käyttäjät voivat tallentaa ja suojata tietoa niin pilvipalveluista, sovelluksista kuin paikallisista ympäristöistä tarvittaessa. Tiedot tallennetaan (AWS S3 n.d.) mukaan ämpäreihin olioina (“data is stored as objects within resources called ‘buckets’” (AWS S3 Features n.d.)). Jatkossa näistä ämpäreistä puhutaan bucket:eina. Amazon S3 palveluun voidaan tallentaa esimerkiksi CloudTrailin keräämät lokit, instansseista saatavat verkkoliikenne lokit tai instanssin sisäisesti keräämät lokit. Amazon S3 tallentaa tietoa niin kauan kuin se sieltä poistetaan, mutta Amazon myös laskuttaa riippuen tiedon määrästä S3 bucket:eista sekä tiedon siirrosta.

2.3.4 AWS CloudTrail

AWS CloudTrail on AWS-ympäristön natiivi palvelu, joka valvoo ja tallentaa tilitoimia AWS-ympäristössä. CloudTrailista voidaan tutkia sekä analysoida kerättyä dataa, esimerkiksi kirjautumistietoja (AWS CloudTrail n.d.). CloudTrail kerää lokia IAM tapahtumista, S3 bucket:eihin tehdyistä toimista, niin lukemisesta, kirjoittamisesta kuin muutoksista, EC2 palvelussa tapahtuvista instanssiin tehdyistä muutoksista, esimerkiksi instanssin käynnistämisestä, sulkemisesta sekä luonnista, Amazon CLI:llä tehdyistä komennoista, sekä Amazon Management Consolessa tehdyistä toimista. CloudTrailin kautta voidaan analysoida ja tarkastella esimerkiksi tietyn käyttäjän toimia.

2.3.5 Amazon EC2

Amazon Elastic Compute Cloud (Amazon EC2) tarjoaa laajimman alustan erilaisille pilvipalveluille niin mobiili applikaatioihin kuin nettisivuihin (Amazon EC2 n.d.). Amazon EC2 on esimerkki IaaS palvelumallin palvelusta, joten mahdollista on valita tarpeisiin sopiva instanssi aina prosessorista käyttöjärjestelmään asti. Koska valittavana on moneen tarpeeseen sopivia alustoja, EC2 onkin yksi Amazonin suosituimpia palveluita. EC2 ympäristöön luodun instanssin sisällä tapahtuvat lokit eivät suoraan ole saatavilla AWS-ympäristöön, vaan ne joudutaan lukemaan instanssin sisältä tai lähettämään instanssista ulos esimerkiksi S3 bucket:iin.

2.4 Forensiikka

Digitaalinen forensiikka tai IT-forensiikka tarkoittaa tiedon hankkimista, säilyttämistä, hakemista sekä esittämistä, joka on käsitelty ja tallennettu sähköisesti (Allen 2005). Digitaalista forensiikkaa voidaan kerätä monista eri lähteistä kuten käyttäjien päätelaitteista (puhelin, tietokone), verkkoliikenteestä sekä pilviympäristöistä (Sammons 2015). Digitaalinen forensiikka koostuukin useista haaroista; tietokoneforensiikka, verkkoforensiikka, mobiililaitteiden forensiikka, tietokantaforensiikka, muistiforensiikka sekä sähköpostiforensiikka. Näiden myötä haasteita digitaaliseen forensiikkaan tuo monet asiat kuten tiedon määrä, erilaiset tallennuslaitteet ja lähteet sekä IP osoitteiden anonyymisyys. (Wazid, Katal, Goudar, Rao 2013). Forensiikka voidaan hyväksikäyttää esimerkiksi tietoturvauhkien tutkimiseen, ”mitä on tapahtunut, kuinka se tapahtui, kuka oli osallisena ja milloin tapahtuma tapahtui” (Årnes 2018).

Pilvipalveluiden forensiikka eroaa itse ylläpidettävästä forensiikasta sillä, että tapahtumat, esimerkiksi applikaatioiden kirjautuminen tehdään pilvipalveluun eikä itse ylläpidettävään ympäristöön. Näin myös lokilähteet muuttuvat sillä lokilähteet eivät olekaan enää omista yrityksen tiloissa ylläpidettävistä servereistä, applikaatioista tai tietokannoista vaan pilvipalvelua tarjoavan yrityksen lähteistä. Tämän vuoksi ymmärrys mitä lokilähteitä pilvipalvelun tarjoajalla on saatavilla, miten sitä voidaan lukea sekä analysoida kasvaa.

2.5 Turvallisuusoperaatiokeskus

Turvallisuusoperaatiokeskus (Security Operation Center (SOC)) on tietoturvatiimi, joka vastaa organisaation turvallisuustason seurannasta sekä analysoinnista. SOC-tiimin tavoitteena on havaita,

analysoida sekä reagoida kyberturvahäiriöihin eri teknologioiden sekä prosessien mukaan. (De Groot, 2020). SOC:issa työskentelee esimerkiksi tietoturva analyytikoita, jotka analysoivat ja reagoivat häiriöihin tutkimalla saatavilla olevia lokilähteitä ja tekemällä niiden perusteella päätöksiä sekä analyysiä. Näin SOC analyytikko tekee digitaalista forensiikkaa havaitusta outoudesta. Jotta analyytikko voi tehdä analyysiä, pitää saatavilla olla tarvittavat lokilähteet sekä ymmärrys mikä ympäristössä on normaalia ja mikä ei. SOC palvelu voi olla yrityksen itsensä ylläpitämä tai palvelua voidaan myydä yrityksille. Suomalaisia palveluntarjoajia SOC:in saralla ovat esimerkiksi Telia Cygate, Elisa Santa Monica, Accenture sekä Nixu (SOC:it Suomessa 2021).

3 Lokilähteiden tutkiminen AWS-ympäristössä

3.1 Lokilähteet

Työn kannalta tärkeiksi lokilähteiksi määräytyi verkkoliikenne lokit, AWS-ympäristön hallintaan liittyvät lokit, sekä AWS-ympäristöön pystytettyjen esimerkiksi virtuaalikoneisiin liittyvät lokit. Nämä lokilähteet antavat hyvän kuvan ympäristössä tehdyistä asioista sekä näillä katetaan suuri osa ympäristössä tapahtuvista tapahtumista.

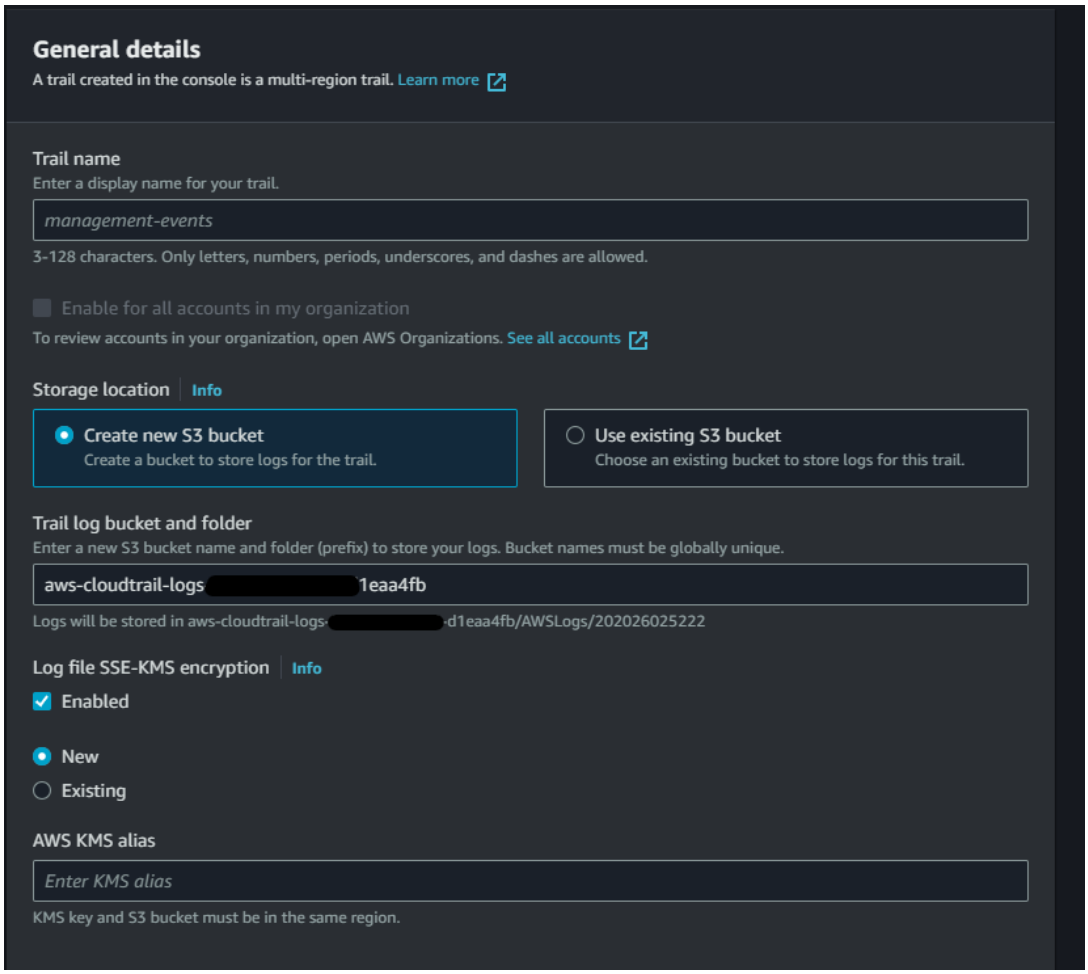
AWS-ympäristön hallintaan liittyvät lokilähteet ovat kirjautumiseen liittyvät lokit, AWS-ympäristöön itsessään tehtyjen muutosten, esimerkiksi virtuaalikoneiden luomiseen, pysäyttämiseen ja poistamiseen sekä yhdistämiseen liittyvät lokit tai uusien ominaisuuksien käyttöönotto sekä poistaminen AWS-ympäristössä sekä käyttäjiin liittyvät lokit esimerkiksi käyttäjien ylläpidolliset lokit (luonti, poistaminen, salasanavaihdot, käyttäjien toimet ympäristössä ja niin edelleen) sekä API aktiviteetit. Kaikkea tätä voidaan seurata Amazon CloudTrailin avulla, joka on AWS-ympäristöön luotu natiivi työkalu tätä varten.

AWS-ympäristön verkkoliikenne lokit saadaan AWS Virtual Private Cloud (AWS VPC) palvelusta, joka kerää jokaisen eri alueen lokit, jos näin halutaan. VPC lokit keräävät pilveen tulevaa ja lähtevää liikennettä, mutta loki analyytikon näkökulmasta on melko kehnoa. Jotkin sovellukset, joita voidaan pystyttää AWS-ympäristöön keräävät verkkoliikennettä omien servereidensä kautta ja nämä serverit voivat antaa parempaa sekä tarkempaa kuvaa sovellukseen tapahtuvista tapahtumista kuin VPC lokit.

Tästä päästään instanssin sisällä tapahtuviin lokeihin, joita ei AWS-ympäristöstä voida suoraan lukea. Instanssien lokit riippuvat siitä, mitä instanssiin on pystytetty, mutta voidaan yleistää, että instanssi lokittaa ainakin käyttöjärjestelmä tasolla systeemilokia (system log), tunnistautumislokia (authentication log) sekä taustaprosessilokia (daemon logs).

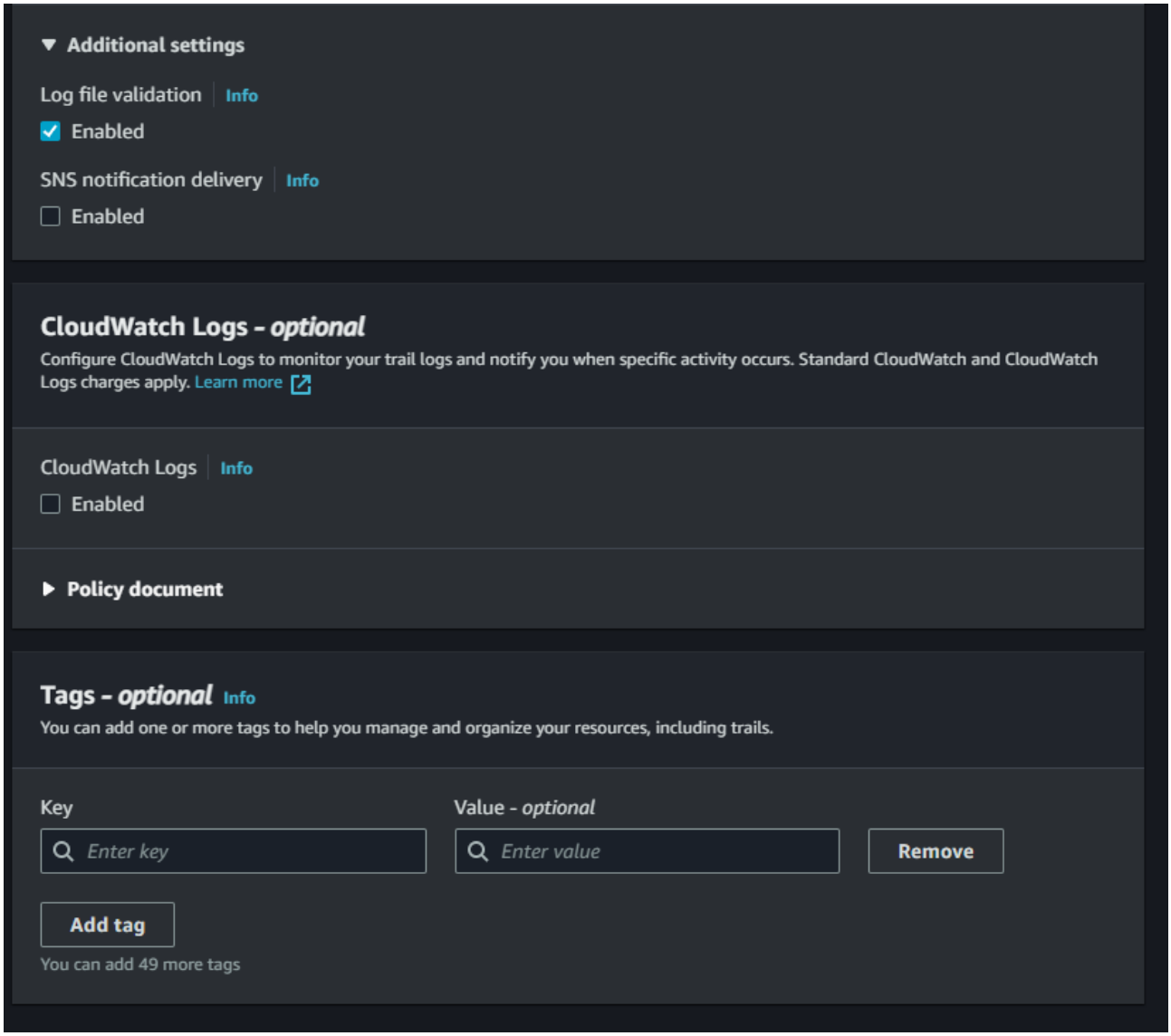
3.1.1 AWS CloudTrail

Identiteetti- ja käyttöoikeushallinta lokeja voidaan tutkia AWS CloudTrailin avulla. CloudTrail on AWS-ympäristön natiivi työkalu lokien keräämiseen sekä tutkimiseen. Ilman CloudTrailia nämä lokit eivät ole saatavilla. Käydään läpi CloudTrailin käyttöönotto sekä tutkitaan millaista lokia CloudTrailista on saatavilla.



Kuvio 1. CloudTrail trailin asetuksia

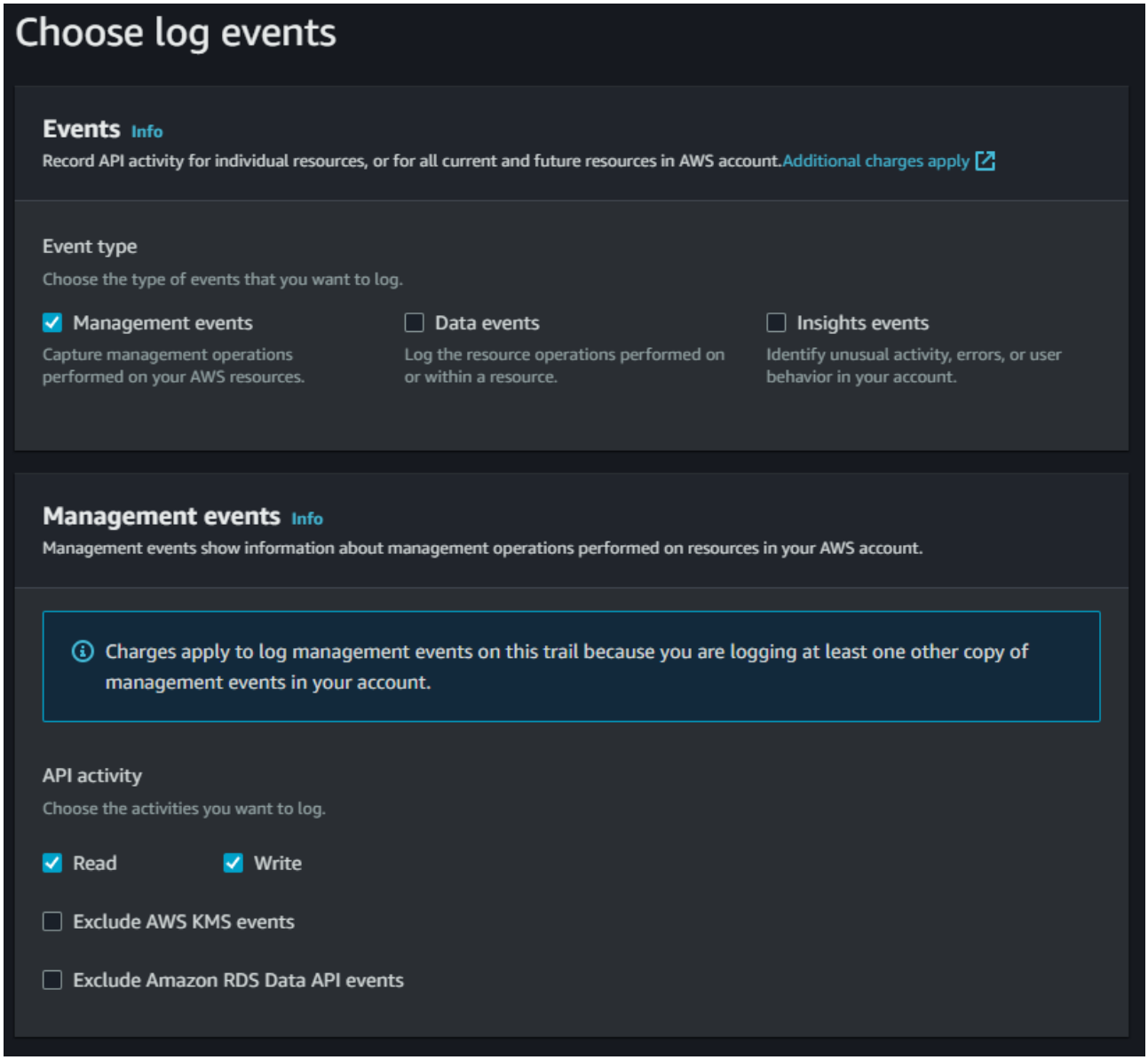
Kuviossa 1 nähdään perinteiset asetukset trailille; nimi, mihin S3 bucket:iin lokit tallennetaan sekä salataanko lokitiedosto. Lokitiedoston salaaminen ei AWS-ympäristössä esiinny haasteena, mutta jos lokitiedostoa siirretään eteenpäin, tämä pitää ottaa huomioon. Salattua tiedostoa ei esimerkiksi kolmannen osapuolen ympäristössä saa auki vaan sen salaus pitää siirtovaiheessa purkaa.



Kuvio 2. CloudTrail lisäasetuksia

Kuviossa 2 on lisää asetuksia trailille. Loki tiedoston validiointi tarkoittaa sitä, että voidaan seurata, tehtiinkö lokitiedostoon muutoksia sen jälkeen, kun se lähetettiin pois AWS-ympäristöstä ja näin turvata tiedoston muuttumattomuus. Halutessaan loki voidaan viedä CloudWatchiin, joka on kes-

kitetty lokien tutkimis- sekä automatisointi palvelu AWS-ympäristössä. Lisäksi trailille voidaan antaa tunnisteita, jotka ovat avain-arvo pareja joita voidaan käyttää trailin sekä S3 bucket:in tunnistamiseen.



Kuvio 3. Trailin lokieventtien valinta

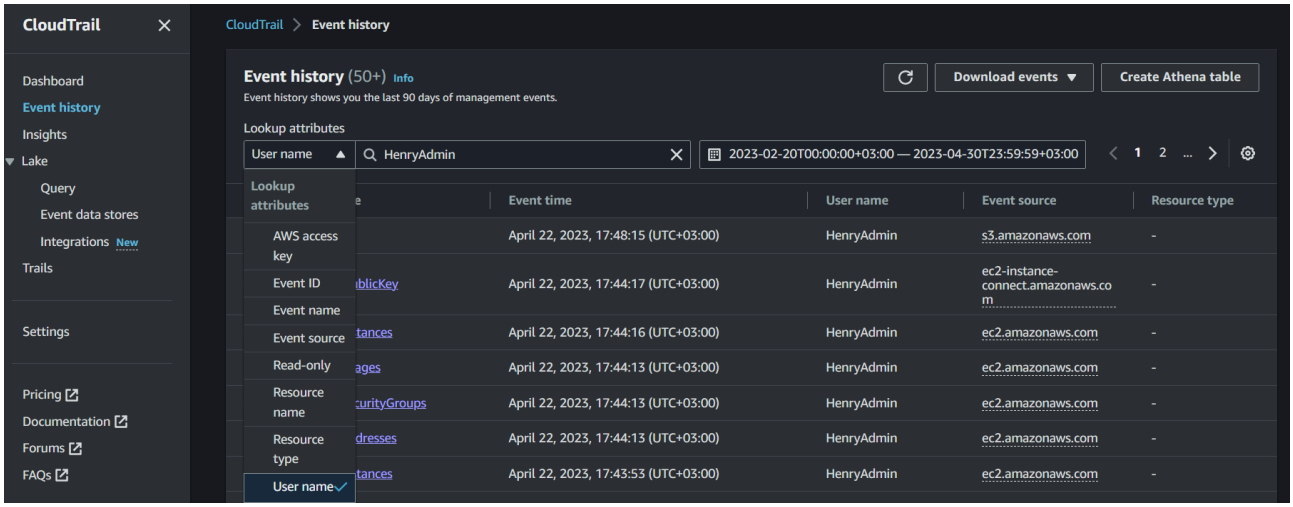
Kun trailin perusasetukset ovat asetettu päästään valitsemaan lokitettavat tapahtumat.

- Management events - Tallentaa AWS resursseille suoritetut hallintatoimet
- Data events – Tallentaa resurssille tai sen sisällä suoritetut toiminnot
- Insights events – Tunnistaa epätavallisen toiminnan tai virheet käyttäjien käyttäytymisessä (vain management eventsien kanssa)

Koska trail tehtiin identiteetti- ja käyttäjähallinta mielessä, valittiin asetus ”management events” sekä ”API (application programming interface – ohjelmointirajapinta) activity” sekä asetuksista valittiin oletukset “Read” ja “Write”. Nämä aktiviteetit lokittavat kaikki käyttäjän tekemät toimet sekä käyttäjään tehdyt toimet. Halutessaan voidaan jättää lokittamatta KMS (key management service) sekä Amazon RDS (hallinnoitu suhdetietokanta muille tietokannoille, esimerkiksi MySQL tai MariaDB) tapahtumat.

CloudTrailin luonnin jälkeen loki on luettavissa sekä tutkittavissa AWS CloudTrail palvelusta. Jotta käyttäjä voi CloudTrailin keräämää lokia lukea, tarvitsee käyttäjälle lisätä oikeat politiikat. On hyvä huomata, että pelkästään CloudTrailiin liittyvät politiikat eivät riitä, vaan S3 bucket:iin johon loki on tallennettu pitää päästä käsiksi. Tämän vuoksi myös lukuoikeus kyseiseen bucket:iin on hyvä lisätä.

CloudTrailista pystyy tutkimaan lokia viimeiseltä yhdeksältä kymmeneltä päivältä, mutta jos loki on tallennettu S3 bucket:iin, lokia voidaan lukea muilla AWS-ympäristön sovelluksilla esimerkiksi AWS Command Line Interfacella (AWS CLI).



Kuvio 4. CloudTrail portaali

Kuviosta 4 nähdään yleiskuva CloudTrail portaalista. Portaalissa voidaan tehdä perusmuotoisia hakuja, riippuen millaista lokia halutaan tutkia. Kuviossa on tehty haku, jossa haetaan kaikki käyttäjän ”HenryAdmin” tekemät toimet ja tapahtumat. Vetovalikosta voidaan vaihtaa hakuparametrejä ja esimerkiksi pelkästään kirjautumislokit voidaan hakea valitsemalla ”Event name” ja hauksi ”ConsoleLogin”. Edellä mainitun kirjautumishaun voi tehdä myös komentokehotteen kautta tekemällä komento ”aws cloudtrail --region us-east-1 lookup-events --lookup-attributes AttributeKey=EventName,AttributeValue=ConsoleLogin”

Kuvio 5. JSON muodosssa olevaa kirjautumislokia

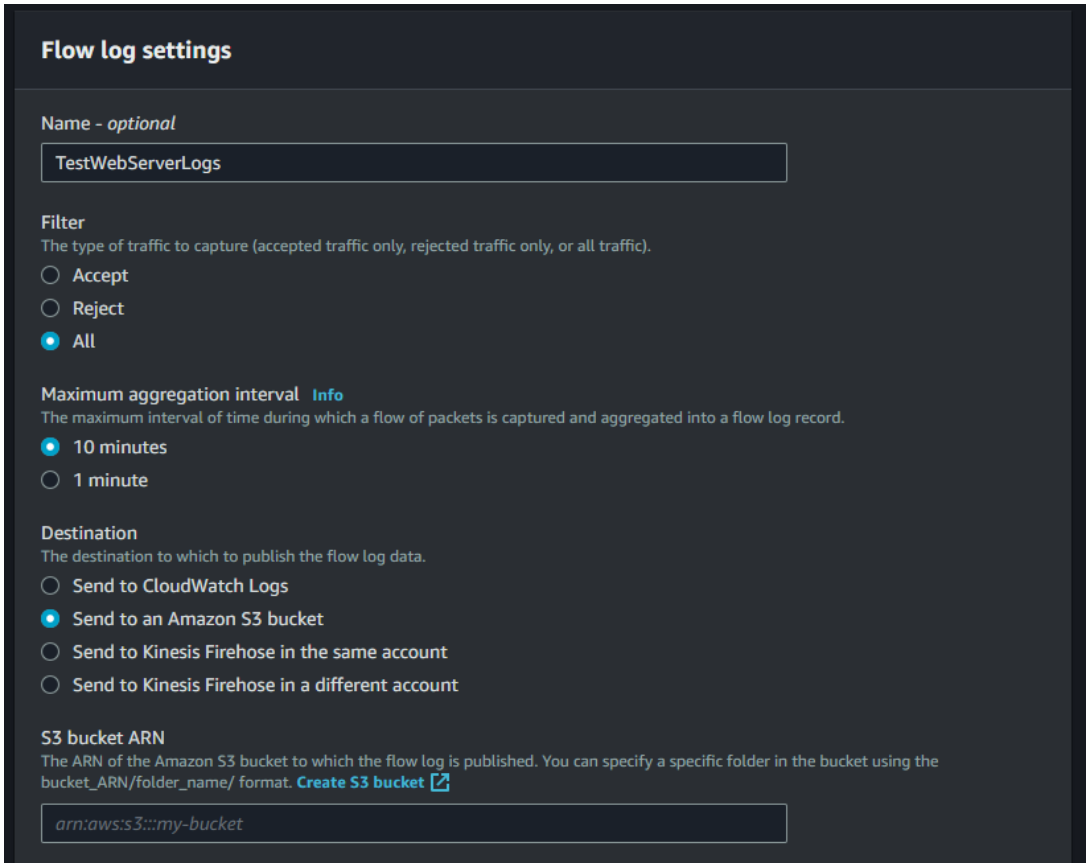
Loki tapahtuman voi myös avata, jolloin saadaan JSON (JavaScript Object Notation) muotoon kirjoitettu tapahtuma lisätietoineen. Osittainen kirjautumistapahtuma on avattu Kuviossa 5 ja tästä nähdään, millaisia tietoja kirjautumistapahtumasta kerätään. Kuviosta 5 voidaan tehdä esimerkiksi johtopäätös, että kirjautuminen on onnistunut ja monivaiheista tunnistusta (Multifactor authentication (MFA)) on käytetty kirjautumisessa.

Syystä tai toisesta kirjautumislokit ovat näkyvissä CloudTrail portaalissa vain, kun alueeksi, jolla toimitaan, valitaan us-east-1. Esimerkiksi eu-central-1 alueella näitä lokeja ei ole saatavilla. AWS

CloudTrail dokumentaation mukaan 22.11.2023 jälkeen on tehty muutos, jonka mukaan IAM tapahtumat tallennetaan alueelle, jossa tapahtumat tapahtuvat eli ”US East (N. Virginia), us-east-1” (AWS Management console sign-in events n.d.). Tämän ei dokumentaation mukaan pitäisi olla ongelma vaan tapahtumien pitäisi CloudTrailiin tulla normaalisti, varsinkin kun CloudTrail on luotu hakemaan lokia monelta alueelta.

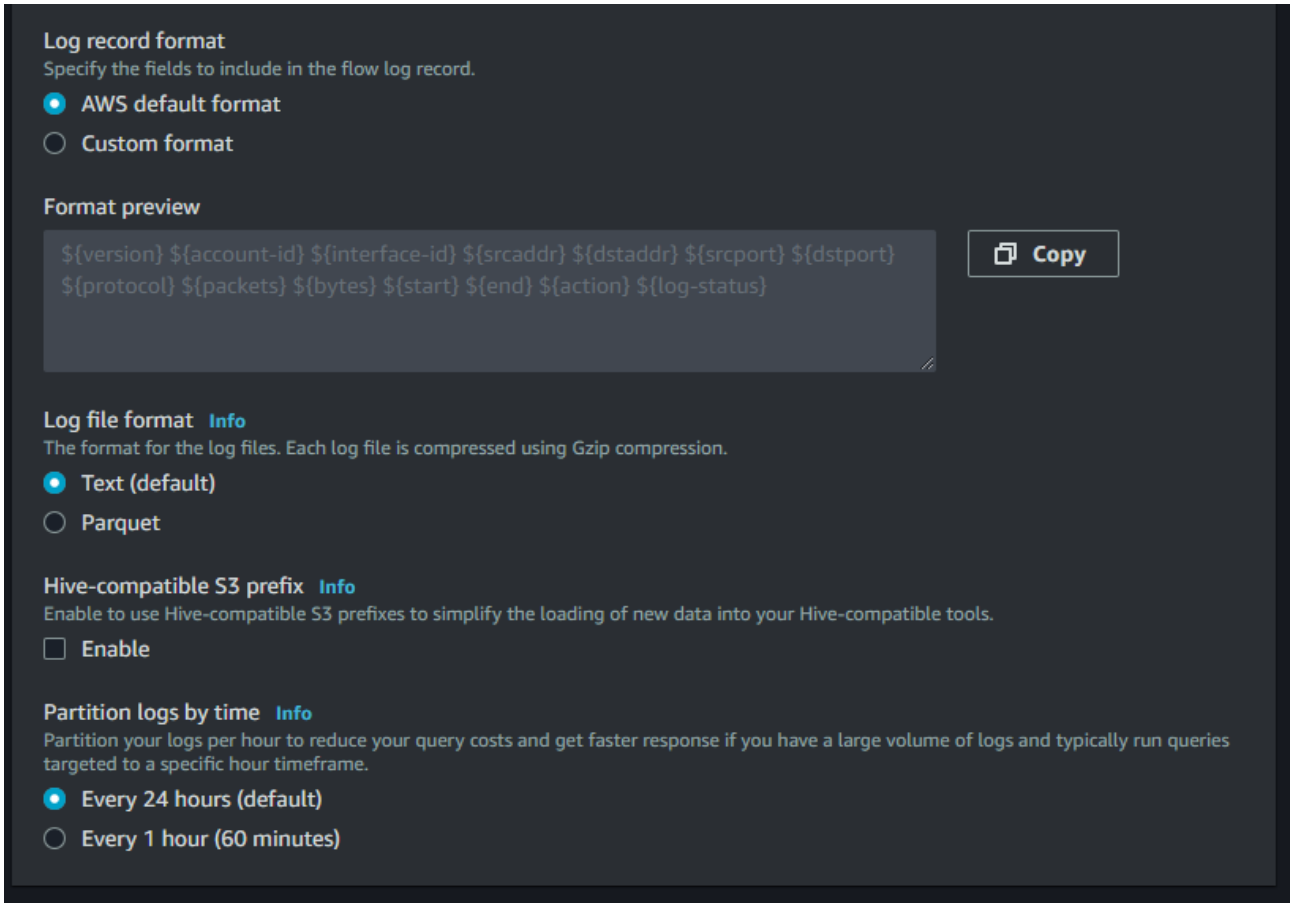
3.1.2 AWS VPC

AWS-ympäristössä jokaisella käyttäjällä on virtuaalinen henkilökohtainen pilvi (Virtual Private Cloud (VPC)) joka on automaattisesti luotu AWS-ympäristön luonnin yhteydessä. Jokaiselle alueelle on oma VPC, joka on hyvä ottaa huomioon ympäristöä pystyttäessä sekä sen konfiguroinnissa. Verkkoliikenne ulkoverkosta omiin instansseihin, pois instansseista sekä pilven sisällä tapahtuva kommunikaatio tallentuu, kun VPC flow lokit konfiguroidaan keräämään tätä lokia. Konfiguroidaan siis VPC Flow loki.



Kuvio 6. Flow lokin asetuksia

Kuviossa 6 nähdään asetuksia flow lokista. Flow lokille annetaan nimi sekä valitaan, halutaanko lokittaa hyväksytty, estetty vai kumpikin liikenne. Valitaan myös, kuinka useasti loki lähetetään sekä mihin kohteeseen. Ensin luotiin flow, joka lähetti lokin S3 bucket:iin ja tämän jälkeen tehtiin identtinen loki, jonka tarkoitus oli lähettää nämä lokit CloudWatchiin.



Kuvio 7. Flow loki formaatti

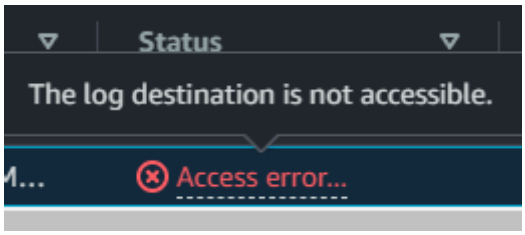
Kuviossa 7 nähdään asetuksia lokin muotoon liittyen. AWS-ympäristön oletusmuoto valittiin, jotta voidaan tutkia tarkemmin millaista lokia flow loki kerää. Lokin muotoon kannattaa kiinnittää huomiota riippuen siitä, kuinka paljon kommunikaatiota kulkee. Aikaisemmin käytiin läpi tekstimuotoisen sekä binäärimuotoisen lokilähteen hyvistä ja huonoista puolista. Parquet muotoon tallennettu loki on binäärimuotoinen loki, jolloin se mahdollistaa isompien lokimäärien siirtämisen nopeasti ja vähentää tallennustilan määrää verrattaen tekstimuotoiseen. Myös lokin osioiminen on hyvä tehdä useasti, jos lokimäärät ovat isoja sillä se nopeuttaa lokin lukemista ja hakemista. VPC flow loki kerää tapahtumasta version, tilin tunnisteen, lähde IP osoitteen, kohde IP osoitteen, lähde

portin, kohde portin, käytetyn protokollan, pakettien määrän, lähetettyjen tavujen määrän, alku-ajan, loppuajan, toiminta, sekä lokitus statuksen. Näistä moni on itsestään selviä, mutta esimerkiksi protokollan ilmaiseminen numerolla sekä ajan ilmaiseminen numerosarjana voivat olla hankalia ymmärtää. Protokollan numero viittaa IANA:n (Internet Assigned Numbers Authority) määrittelemään protokollien listausmalliin, jossa jokaiseen protokollaan viitataan numerona. Esimerkkeinä numero seitsemäntoista, joka tarkoittaa UDP:hen (User Datagram Protocol) sekä numero kuusi, joka tarkoittaa TCP:tä (Transmission Control Protocol). Alku- ja loppuajat ovat Unix aikaa, joka tarkoittaa sitä, kuinka monta sekuntia on mennyt ajankohdasta 1. tammikuuta 1970 kello 0.00.00 UTC. Taulukossa 2 nähdään esimerkki millaista tietoa flow loki kerää ja lokittaa.

Taulukko 2. Flow loki esimerkki S3 bucket:ista

account-id	interface-id	srcaddr	dstaddr	srcport	dstport	protocol	packets	bytes	start	end	action	log-status
x	eni-063e25fdcdb0b64fd	178.63.9.212	172.31.22.36	123	49653	17	1	76	1682952737	1682952796	ACCEPT	OK
x	eni-063e25fdcdb0b64fd	91.189.94.4	172.31.22.36	123	48742	17	1	76	1682952737	1682952796	ACCEPT	OK

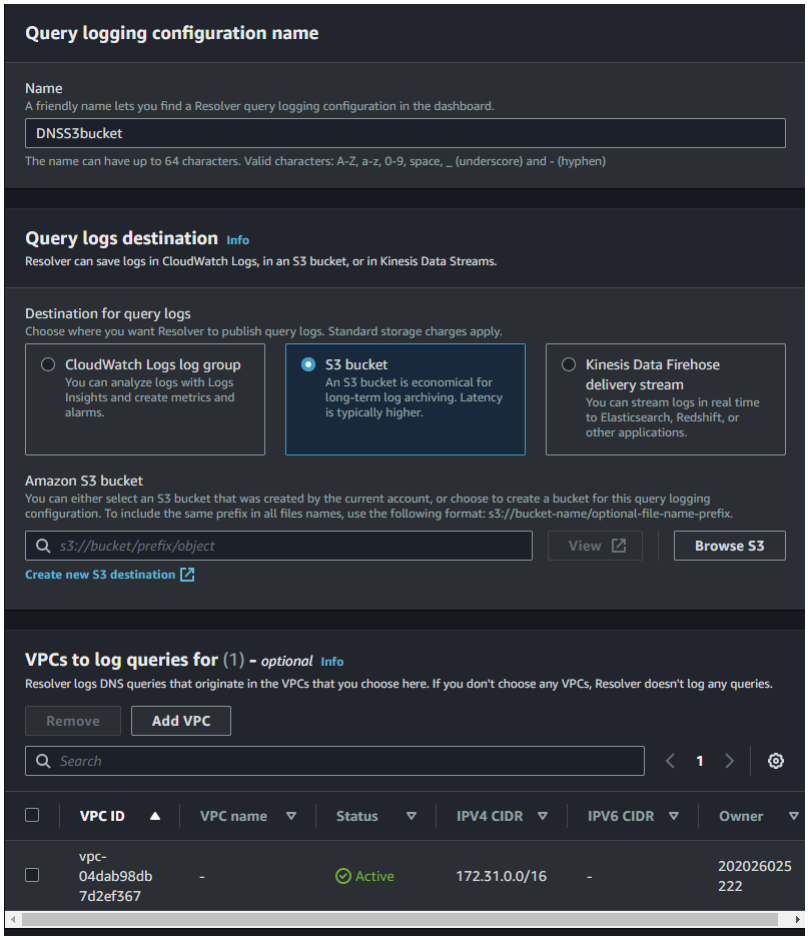
Flow loki yritettiin viedä suoraan CloudWatchiin seuraten dokumentaatiota (VPC Flow log n.d.), mutta jostain syystä tämä epäonnistui.



Kuvio 8. Flow log CloudWatchiin virhe

Kuviossa 8 nähdään, että ongelmaksi muodostui se, että kohteeseen ei saatu yhteyttä. Tämä ongelma ei ratkennut, vaikka roolitus, jonka CloudWatch integraatio vaati, tarkistettiin useaan otteeseen sekä annettiin monia dokumentaation mukaan tarpeettomia politiikkoja käytetylle roolille IAM portaali kautta. CloudWatch sekä VPC ovat myös samalla alueella, joten tämänkään ei pitäisi ongelmaksi koitua. Taulukossa 2 näkyvä loki on siis haettu S3 bucket:ista, vaikka halu tutkia lokia AWS ympäristön natiivi sovelluksesta CloudWatch oli.

Amazonilla on palvelu myös DNS (Domain Name System) kyselyjen lokittamiselle. Amazon Route 53 toimii DNS-palveluna AWS-ympäristössä tehdyille DNS-kyselyille ja tämä voidaan konfiguroida keräämään tapahtuvaa DNS kommunikaatiota. DNS-palvelu muuttaa käyttäjän antaman verkkotunnuksen IP-osoitteeksi, joka mahdollistaa kommunikaation verkossa. Lokitus saadaan käyttöön, kun konfiguroidaan Route 53:n resolveri lokittamaan ympäristössä tapahtuvat tiedustelut.



Kuvio 9. Route 53 lokitus asetuksia

Kuviosta 9 nähdään kaikki kysely lokin asetukset. Loki voidaan tallentaa suoraan CloudWatchiin johon VPC lokeja ei edellä saatu siirtymään, S3 bucket:iin tai suoraan esimerkiksi Elasticsearch:iin jakeluvirran avulla. Lokin tallennuspaikaksi valittiin S3 bucket, johon loki saatiin tallennettua. Ympäristöksi valittiin VPC, jolle myös instanssit luotiin myöhemmin.

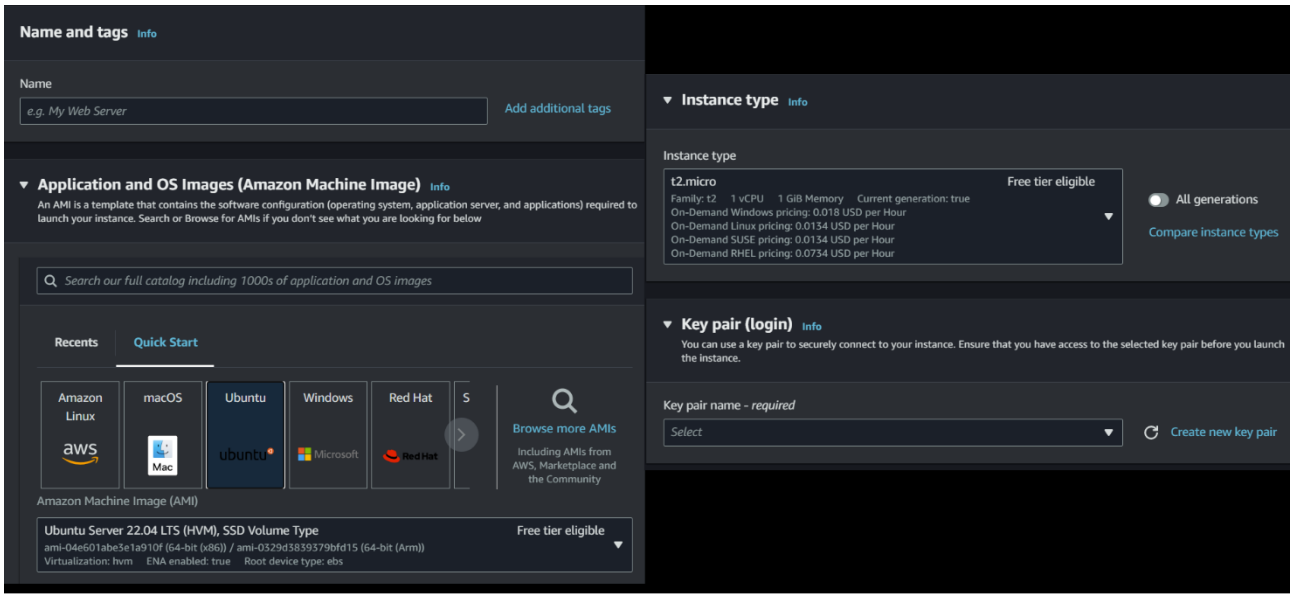

```
2023-05-24T19:31:25.000+03:00          {"version":"1.100000","account_id":'

{
    "version": "1.100000",
    "account_id": "[redacted]",
    "region": "eu-central-1",
    "vpc_id": "vpc-04dab98db7d2ef367",
    "query_timestamp": "2023-05-24T16:31:25Z",
    "query_name": "google.com.",
    "query_type": "AAAA",
    "query_class": "IN",
    "rcode": "NOERROR",
    "answers": [
        {
            "Rdata": "2a00:1450:4001:80e::200e",
            "Type": "AAAA",
            "Class": "IN"
        }
    ],
    "srcaddr": "172.31.22.36",
    "srcport": "44336",
    "transport": "UDP",
    "srcids": {
        "instance": "i-087077dee59519cee"
    }
}
```


Kuvio 10. Loki esimerkki DNS lokista CloudWatchista

Kuviossa 10 nähdään lokitapahtuma, jossa päätelaite teki kyselyn kohteeseen google.com. Lokista saatavan tiedon perusteella voidaan sanoa kuka kyselyn teki, millainen kysely tehtiin sekä vastauksena saatiin google.com:in IPv6 -osoite. Muiden lokitapahtumien tutkinta näyttäisi myös IPv4 -osoitteen, mutta se ei kuvioon tälläkertaa valikoitunut. Syystä tai toisesta tämän lokilähteen viminen CloudWatchiin onnistui ilman ongelmia ja näin lokin tutkiminen onnistuu sujuvasti myös AWS ympäristöstä.

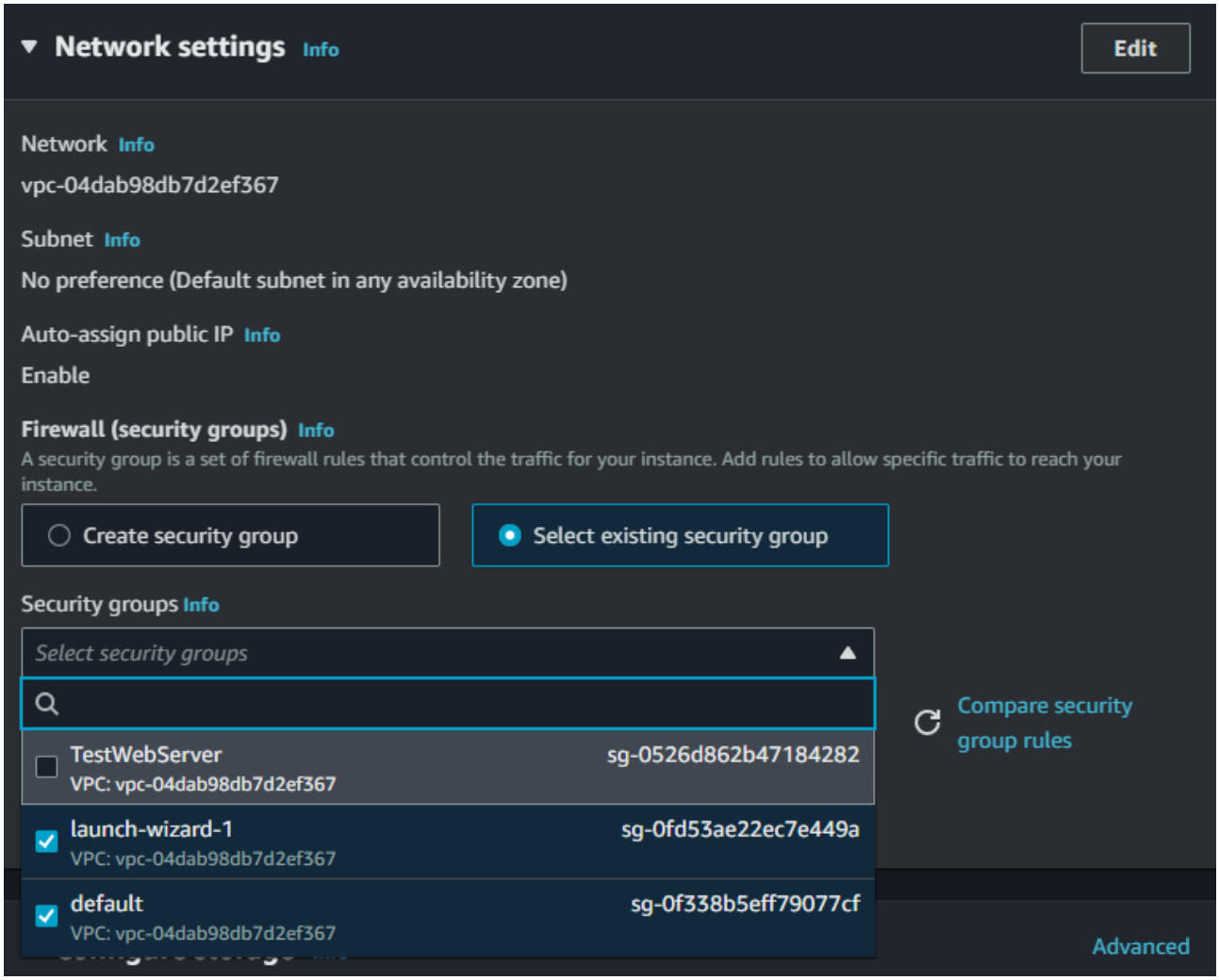
3.1.3 AWS Instassi lokit

AWS instansseihin tehtävät muutokset käyttäjien toimesta AWS-ympäristössä lokittuvat CloudTraililla. CloudTrail ei kuitenkaan näe instanssin sisälle, joten instansseissa tapahtuvat toimet sekä tapahtumat on haettava muuta kautta. Jotta instanssien tuottamia lokeja voidaan tutkia, täytyy AWS-ympäristöön luoda instanssi. Luodaan Amazon EC2 instanssi (Ubuntu virtuaalikone) jolle lisätään WordPress, jotta voidaan tutkia VPC flow lokin sekä http serverin antaman lokin eroavaisuuksia. Kyseinen instanssi on esimerkki IaaS ympäristöstä, jossa pilvipalvelusta ostetaan laskentatehoa, tallennustilaa, verkotusta sekä muita tarpeellisia resursseja.



Kuvio 11. Instanssin asetuksia

Kuviossa 11 annettiin instanssille nimi ”TestWebserver2” sekä valittiin Ubuntu virtuaalikone instanssin pohjaksi. Tämän webserverin oli tarkoitus tuottaa perusmuotoista lokia, jotta saadaan ymmärrys millaista lokia on saatavilla. Instanssi tyypissä voidaan valita tarvittava prosessointi teho, joka on normaalia IaaS palvelulle. Pystyttäessä instanssia, ei koettu tarvetta suuren virtuaalikoneen pystytykselle, jonka vuoksi prosessointi teholle valittiin pienin ja ilmaisuuden täyttävä vaihtoehto. Instanssille luotiin myös avainpari ”TestWebServer”, joka mahdollistaa instanssiin kirjautumisen suoran AWS-ympäristöstä.



Kuvio 12. Instanssin internet asetukset

Kuviossa 12 valitaan mihin VPC ympäristöön instanssi luodaan. Luonnin yhteydessä AWS ehdotti suoraan saman alueen sisällä olevaa VPC:tä missä työskenneltiin. Instanssille valittiin turvaryhmiksi, jotka ovat palomuurisääntöjä, AWS-ympäristön automaattisesti luomat ”launch-wizard-1“, joka kuuntelee TCP protokollalla mistä tahansa IP osoitteesta tulevaa liikennettä portissa 22 sekä lähettää liikennettä mihin tahansa IP osoitteeseen mistä tahansa portista sekä ”default” joka kuuntelee kaikkea sisään tulevaa liikennettä sekä lähettää liikennettä mihin tahansa.

Kun instanssi luotiin, asennettiin sille WordPress ja tämän jälkeen lähdettiin tutkimaan millaista lokia instanssista on saatavilla. Instanssin sisällä tapahtuvat tapahtumat eivät näy AWS-ympäristölle millään tavalla. VPC flow loki lokittaa kyllä verkkoliikennettä, mutta instanssin sisällä

tapahtuvat komennot sekä erilaiset palvelujen käynnistämiset ja sammuttamiset eivät ulkopuolelle näy. Ubuntu lokittaa käyttöjärjestelmä tasolla esimerkiksi systeemilokia (system log), tunnistautumislokia (authentication log) sekä taustaprosessilokia (daemon logs). Yksi esimerkki saada kyseiset lokilähteet AWS-ympäristöön on lähettää ne suoraan S3 bucket:iin ja tämän voi tehdä AWS CLI työkalun avulla. AWS Command Line Interface (AWS CLI) on työkalu, jonka avulla voidaan kommunikoida AWS-ympäristön kanssa komentoriviltä. Se antaa samat mahdollisuudet komentoihin kuin selainpohjainen AWS CloudShell joka on AWS-ympäristön oma CLI. Jotta AWS CLI saadaan lähettämään lokia instanssilta, AWS CLI pitää asentaa instanssiin sekä konfiguroida se toimimaan AWS-ympäristön kanssa. Asennus tapahtui Amazonin “Installing or updating the latest version of the AWS CLI” dokumentaation perusteella. Kun AWS CLI on asennettu, pitää se konfiguroida kommunikoimaan oikean AWS-ympäristön kanssa komennolla “aws configure”. Konfiguroinnissa on hyvä ottaa huomioon millaisia oikeuksia on tilillä, jota käytetään kommunikoimaan AWS-ympäristöön CLI:n avulla ja millaisia oikeuksia siihen tarvitaan. Kun tämä on konfiguroitu, voidaan instanssista lähettää lokit S3 bucket:iin komennolla “aws s3 cp /var/log/<your-log-file> s3://<your-bucket-name>/".

Esimerkkinä instanssin lokista voidaan tutkia instanssiin asennetun Apache http serverin lokia, joka kerää lokia verkkoliikenteestä web-palvelimeen. Esimerkki lokia on taulukossa 3 ja lokia verrattaessa VPC flow lokiin (taulukko 2) huomataan, että Apache kerää enemmän tietoa tapahtumasta kuin VPC. Toki Apache ottaa huomioon vain serveriin tehdyn kommunikaation, kun taas VPC flow loki kaiken kommunikaation VPC ympäristöön.

Taulukko 3. Apache lokia

time	time-zone	host:port	client	identity of client	identity of user	HTTP request	HTTP status code	bytes	referrer	user-agent
[15/May/2023:00:11:39	+0000]	ip-172-31-22-36.eu-central-1.compute.internal:80	1.14.7.100	-	-	HEAD /Core/Skin/Login.aspx HTTP/1.1	301	314	-	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/106.0.0.0 Safari/537.36
[15/May/2023:00:11:40	+0000]	Sama kuin yllä	1.14.7.100	-	-	HEAD /Core/Skin/Login.aspx HTTP/1.1	404	293	http://3.76.212.141:80/Core/Skin/Login.aspx	Sama kuin yllä
[15/May/2023:00:49:40	+0000]	Sama kuin yllä	104.167.222.194	-	-	GET /.env HTTP/1.1	404	41848	-	Sama kuin yll’
[15/May/2023:00:49:41	+0000]	Sama kuin yllä	104.167.222.194	-	-	POST / HTTP/1.1	200	8783	-	Sama kuin yllä
[15/May/2023:01:01:21	+0000]	Sama kuin yllä	135.125.246.110	-	-	POST / HTTP/1.1	200	8783	-	Sama kuin yllä

Instanssien lokit voidaan automatisoida lähetettäviksi AWS-ympäristöön sekä S3 bucket:iin esimerkiksi cron -ajastuspalvelulla. Komentona käytettiin “0 * * * * aws s3 sync /var/log/<your-log-file> s3://<your-bucket-name>/” jolla synkronoidaan lokilähde joka tunti. Sama voidaan tehdä muillekin instanssin lokilähteille. ”Sync” komennossa on hyvä ottaa huomioon, miten instanssin lokilähde ylläpitää lokeja sillä komento kopioi rekursiivisesti uudet sekä päivitetyt tiedostot lähdehakemistosta kohteeseen. Jos kansiosta löytyy myös muita tiedostoja, ”sync” komento kopioi myös ne.

4 Tulokset sekä pohdinta

Tutkinnat tarkoituksena oli tutustua siihen, millaisia lokilähteitä AWS-ympäristössä on saatavilla, miten ne saadaan käyttöön sekä mitä asetuksia lokilähteille annetaan. Identiteetti- sekä käyttöoikeus lokien kanssa päädyttiin konfiguroimaan Amazon CloudTrail, joka keräsi kyseistä lokia todella kattavasti. IAM lokia pystyi myös tutkimaan tarkasti AWS-ympäristön natiiveilla sovelluksilla, joten IAM lokien suhteen työ onnistui loistavasti ja lokilähteen vienti CloudWatchiin onnistui myös, vaikka tähän ei työssä muuten puututtu. Internet lokia saatiin kerättyä myös yllättävän hyvin, vaikkakin olettamus että lokilähteistä saatava loki olisi kattavampaa ei täyttynyt. Harmittamaan myös jäi VPC loki ja sen ongelmat lähettäessä lokia CloudWatchiin. Myös instansseista saataviin lokilähteisiin tutustuttiin ja näitä saatiin tuotua AWS-ympäristöön. Kuitenkaan näihin ei löytynyt hyvää tapaa tutkia natiiveilla sovelluksilla tai oikeaa tapaa ei työn teon aikana löydetty. Ohjeet kuinka instanssien lokia voidaan tuoda instansseista ulos kuitenkin tehtiin, joten näiden lokien osalta päästiin ainakin puoleenväliin halutusta lopputuloksesta. Jatkokehityksenä tulisi tarkastella lokitapahtumien vientiä keskitettyyn lokienhallintajärjestelmään, jossa erityyppisiä lokeja voidaan tutkia keskitetysti. Tämä oli alun perin tarkoitus työssä, mutta siihen ei päästy.

Tutkinnan alussa AWS-ympäristöstä ei aikaisempaa kokemusta ollut. Tämä yhdistettynä omaan oppimistapaan, joka on ympäristön tutkimista ennen dokumentaation lukua sekä ympäristössä tapahtuvaa ongelmien ratkaisua kun ongelmia kohdataan, hidasti työn tekemistä. Ongelmat realisoituivat esimerkiksi CloudTrailin pystytyksen jälkeen, kun huomasin, että kirjautumislokit eivät olleet syystä tai toisesta saatavilla. Pitkän tutkinnan sekä dokumentaation läpikäynnin jälkeen huomattiin, että kirjautumislokit ovat saatavilla, mutta ainoastaan jos alueeksi on valittuna “us-east-1". Vaikka CloudTrailin asetukset olivatkin oikein ja keräsivät lokia monesta alueesta samanaikaisesti sekä S3 bucket:in asetukset hyväksyivät kirjoittamisen mistä tahansa alueesta eivät kirjautumislokit löytäneet tietään CloudTrailin palveluun. Tästä en johtopäätökseen päässyt missä vika, oliko

kenties ilmaisversiossa toiminto pois vai löytyikö ympäristöstä bugi. Kuitenkin Amazonin dokumentaation mukaan kyseiset ”ConsoleLogin” tiedot olisi pitänyt löytyä. Myös muita ongelmia, kuten VPC lokien vienti CloudWatchiin huomattiin eikä näihin syitä löytynyt.

Lähteet

Allen, W.H. 2005. Artikkeli “Computer Forensics”. Viitattu 6.9.2022. https://janet.finna.fi/, IEEE.

Amazon AWS. N.d. Artikkeli "What is AWS". Viitattu 14.2.2023. https://aws.amazon.com/what-is-aws

Amazon CloudComputing. N.d. Artikkeli “What is cloud computing”. Viitattu 23.442023. https://aws.amazon.com/what-is-cloud-computing/

Amazon what is IaaS. N.d. Artikkeli “What is IaaS”. Viitattu 24.4.2023. https://aws.amazon.com/what-is/iaas/

AWS CloudTrail. N.d. Amazon dokumentaatio. Viitattu 20.2.2023. https://aws.amazon.com/cloudtrail

AWS EC2. N.d. Amazon dokumentaatio. Viitattu 15.2.2023. https://aws.amazon.com/ec2

AWS IAM. N.d. Amazon dokumentaatio. Viitattu 17.2.2023. https://aws.amazon.com/iam

AWS Management console sign-in events. N.d. Amazon dokumentaatio. Viitattu 20.5.2023. https://docs.aws.amazon.com/awscloudtrail/latest/userguide/cloudtrail-event-reference-aws-console-sign-in-events.html

AWS S3. N.d. Amazon dokumentaatio. Viitattu 14.2.2023. https://aws.amazon.com/s3

AWS S3 Features. 2023. Amazon dokumentaatio. Viitattu 1.5.2023. https://aws.amazon.com/s3/features

Chen, L., Takabi, H. 2019. Security, privacy and digital forensics in the cloud. Singapore: John Wiley & Sons. Viitattu 6.9.2022. https://janet.finna.fi/, EBSCOhost Ebooks.

De Groot, J. 2020 "What is a Security Operations Center (SOC)?". Blogi kyberturvallisuuskeskuksista. Viitattu 9.5.2023. https://www.digitalguardian.com/blog/what-security-operations-center-soc

Elisa Santa Monica. N.d. Elisa Santa Monica Oy:n kotisivut. Viitattu 24.5.2023. https://www.elisasantamonica.fi/

Elisa Santa Monica taloustiedot. N.d. Finderin verkkosivu. Viitatu 24.5.2023. https://www.finder.fi/Tietoliikennepalvelut+tietoliikennelaitteet/Elisa+Santa+Monica+Oy/Helsinki/yhteystiedot/920995

Kent, K., Souppaya, M. 2006. NIST SP 800-92. Guide to Computer Security Log Management. Viitattu 2.5.2023. https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-92.pdf

Mell, P., Grance, T. 2011. NIST SP 800-145. The NIST Definition of Cloud Computing. Viitattu 20.4.2023. https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf

Microsoft Azure. N.d. Artikkeli "What is cloud computing". Viitattu 14.2.2023. https://azure.microsoft.com/en-us/resources/cloud-computing-dictionary/what-is-cloud-computing

Sammons, J. 2014. The basics of digital forensics: the primer for getting started in digital forensics. Viitattu 6.9.2022. https://janet.finna.fi/, Skillsoft Books.

SOC:it suomessa. 2021. Verkkosivu, johon kerätty Suomen SOC toimijoita. Viitattu 24.5.2023. https://csoc.fi/

Todd, B. 2017. White Paper "Creating a logging infrastructure". Viitattu 2.5.2023. https://www.sans.org/white-papers/38130/

VPC Flow log. N.d. Amazonin dokumentaatio VPC flow lokista. Viitattu 10.5.2025. https://docs.aws.amazon.com/vpc/latest/userguide/flow-logs-cwl.html

Wazid, M., Katal, A., Goudar, R.H., Rao, S. 2013. Konferenssijulkaisu “Hacktivism Trends, Digital Forensic Tools and Challenges: A Survey”. Viitattu 6.9.2022. https://janet.finna.fi/, IEEE.

Årnes, A. 2018. Digital forensics: an academic introduction. Viitattu 6.9.2022. https://janet.finna.fi/, Skillsoft Books.