Jesse Kuusela

Tiedostopalvelinten käytäntöjen kehittäminen

Opinnäytetyö

Tekniikan ammattikorkeakoulututkinto

Tieto- ja viestintätekniikan koulutus

2022

Kaakkois-Suomen ammattikorkeakoulu

Kaakkois-Suomen ammattikorkeakoulu

Tutkintonimike	Insinööri (AMK)
Tekijä/Tekijät	Jesse Kuusela
Työn nimi	Tiedostopalvelinten käytäntöjen kehittäminen
Vuosi	Lokakuu 2022
Sivut	46 sivua
Työn ohjaaja(t)	Vesa Kankare

TIIVISTELMÄ

Kyberturvallisuuden kehittyessä myös kyberhyökkäykset adaptoituvat uusiin teknologioihin nopeasti. Yrityksen täytyy pysyä ajan tasalla kehittyvän teknologian kanssa, jotta se ei joudu hyökkäyksien uhriksi. Tiedostopalvelimet ovat kriittisimpiä suojelun kohteita, sillä ne yleensä sisältävät suuren osan yrityksen arkaluontoisesta tiedosta. Kaapatut käyttäjätilit ovat usein syynä arkaluontoisen tiedon vuotamiselle.

Toimeksiantajan tiedostojakojen ja käyttäjäryhmien eri vastuuhenkilöitä haastateltaessa ilmeni, että yrityksen tiedostopalvelimien suojaamiseen ei ole otettu käyttöön kaikkia menetelmiä, joita moni saattaisi tulkita tärkeinä vaatimuksina. Tämän lisäksi haastateltavat halusivat kyseenalaistaa myös jo toimeksiantajan toiminnassa olevia käytäntöjä. Nämä haastattelut loivat tavoitteen koventaa toimeksiantajan tiedostojakoja sekä periaatetasolla että käytännön tasolla.

Työ oli aluksi täysin teoriapohjainen, mutta myöhemmin todettiin tarpeelliseksi myös testata erilaisia työkaluja. Jotta työkaluja päästiin testaamaan, työssä hyödynnettiin Kaakkois-Suomen ammattikorkeakoulun virtuaalista testiympäristöä. Työ toteutettiin interventionistisenä kehittämistutkimuksena.

Testiympäristössä testattiin kahta työkalua. Toinen niistä monitoroi ja analysoi käyttöoikeuksia, kun taas toisella työkalulla skannattiin arkaluontoista tietoa tiedostojaoista. Testien onnistuneista tuloksista voidaan todeta, että niiden käyttöönotto voisi olla toimeksiantajalla hyödyksi.

Asiasanat: tiedostopalvelimet, kyberturvallisuus, käyttäjäryhmät, tiedostot, Windows

South-Eastern Finland University of Applied Sciences

Degree	Bachelor of Engineering
Author (authors)	Jesse Kuusela
Thesis title	Development of file server practices
Time	October 2022
Pages	46 pages
Supervisor	Vesa Kankare

ABSTRACT

The continuous development of cybersecurity also brings more capable cyber attacks. Companies have to adapt to the ever-changing cybersecurity requirements in order to avoid becoming a victim of a cyber attack. File servers are one of the most critical assets to protect as they usually store most of the company's sensitive information. Hacked user accounts are often the cause for sensitive information leakage.

Interviewing the commissioner personnel revealed that some key aspects of a recommended cybersecurity strategy are missing from their file servers. One of the interviewees also suggested that their current practices in use should be looked into to make sure that they are following best practices. After the interviews were conducted, it was agreed that the objective would be to harden the company's file shares.

The original plan for this thesis was to keep everything on a theoretical level. However, it was later deemed best to also try out various tools. For this, a test environment was created to the Xamk virtual laboratory. This thesis was conducted using the interventionist research method.

There were two tools tested in the test environment. One of them monitored and analyzed access rights, while the other one scanned for sensitive information in file shares. Successful tests in the test environment prove, that their deployment could prove useful for the commissioner.

Keywords: file servers, cybersecurity, user groups, files, Windows

SISÄLLYS

1 JOHDANTO

Teknologian kehittyessä ja maailman digitalisoituessa yritysten varastoiman datan määrä on kasvanut. Datan lisääntyessä sen hallinta muuttuu haastavammaksi ja varastointi vaatii enemmän suunnittelua.

Tiedostopalvelimilla taataan yhteinen keskitetty varasto, jonka sisältöön käyttäjät pääsevät käsiksi liityttyään verkkoon. Konfiguroimalla käyttäjäryhmiä huolellisesti voidaan ylläpitää turvallista ympäristöä, jossa käyttäjät voivat nähdä ja hallita juuri heille tarpeellisia tiedostoja.

Kasvavissa yrityksissä voi kuitenkin syntyä suuria määriä käyttäjäryhmiä, joiden ylläpito vaatii työtä. Mikäli tiedostohakemistoja kartoitetaan ilman yhteistä toimintamallia, niiden huoltaminen on työläämpää. Luonnollisesti myös tietoturvariskit kasvavat yrityksen ja ryhmien laajentuessa.

Kuten käyttäjäryhmien, myös käyttöoikeuksien määritteleminen muuttuu monimutkaisemmaksi työksi käyttäjäkunnan kasvaessa. Jos käyttäjäryhmien siistimistä on laiminlyöty, virheelliset käyttöoikeudet vaarantavat arkaluontoisen tiedon leviämisen vääriin käsiin. Pelkästään käyttäjien käyttöoikeuksien rajaaminen ei poista tiedostopalvelimien tietoturvariskejä, sillä käyttäjät voivat aiheuttaa vahinkoa yrityksen tiedostojärjestelmiin myös heille hyvästä syystä annetuilla käyttöoikeuksilla. Tästä syystä käyttäjien toimintaa täytyy pystyä rajaamisen lisäksi myös monitoroimaan.

Kuten monia muita tietotekniikan puolia, myöskään tiedostojärjestelmiä ei pystytä koventamaan täydellisesti. Tiedostopalvelimissa tulee aina olemaan tietoturva-aukkoja, mutta niiden määrää ja vaikutusta voidaan minimoida selvillä toimintamalleilla sekä työkaluilla, joiden avulla käyttäjien toimintaa ja käyttöoikeuksia voidaan hallita ja monitoroida.

Tiedostojen turvaaminen on tarpeellista, sillä arkaluontoisen tiedon karatessa yritykselle ei ole vaarana pelkästään taloudelliset menetykset, vaan myös maineen vaurioituminen. Tiedostojärjestelmien tietoturvariskit on onneksi selvästikin huomioitu maailmalla, sillä monet eri teknologiayritykset tarjoavat tutkittuja

parhaita käytäntöjä dokumentaatioissaan. Tiedostojärjestelmille on myös kehitetty monia eri työkaluja helpottamaan järjestelmänvalvojien elämää.

Tämän opinnäytetyön tarkoitus on kehittää toimintamalli tiedostopalvelinten konfiguraatiolle, joka pyrkii huomioimaan sekä käytännöllisyyden että turvallisuuden niiden ristiriidasta huolimatta. Toimeksiantajan IT-infrastruktuuri sisältää pääosin Windows Server -palvelimia, joten työssä käsitellään sen käyttämää NTFS-tiedostojärjestelmää ja sen käyttöoikeuksia. NTFS-käyttöoikeuksille ja yleisille käyttöoikeuksien jakeluperiaatteille tutkitaan parhaita käytäntöjä. Työssä testataan myös työkaluja, joilla voidaan hallita tiedostopalvelimia ja käyttäjäryhmiä. Päätavoitteena on yksinkertaistaa tiedostopalvelimien ylläpitoa ja samalla minimoida niiden tietoturvariskit.

2 TUTKIMUSASETELMA

Toimeksiantajan tiedostopalvelimista ja tiedostojaoista vastaavat henkilöt ovat osoittaneet huolenaiheita heidän ympäristöstään. Ajan kuluessa eri työntekijät ovat rakentaneet käyttäjäryhmiä ja tiedostojakoja omilla tavoillaan ja se näkyy muun muassa käyttöoikeuksien jakelutavoissa sekä ylimääräisissä ryhmissä, jotka tuottavat päällekkäisiä käyttöoikeuksia. Arkaluontoista dataa halutaan suojata, mutta käyttäjien työnteosta ei kuitenkaan haluta tehdä turhan hankalaa. Tiedostopalvelimien ja käyttäjäryhmien hallintaa helpottavia työkaluja ei ole ehditty tutkimaan. Mikäli testatut työkalut täyttävät toimeksiantajan vaatimukset, niiden käyttöönottoa voidaan ehdottaa.

Näistä aiheista herää kysymykset:

- Mitä toimenpiteitä ylläpidon helpottaminen vaatii?
- Miten käyttäjäryhmiä saadaan järjesteltyä nyt ja tulevaisuudessa?
- Miten palvelinympäristön käytännöllisyyttä ja turvallisuutta tasapainotetaan?
- Mitä mahdollisuuksia käyttäjäryhmien ja tiedostojärjestelmien hallintaan tarkoitetut työkalut tarjoavat?

Tutkimusongelmalle harkittiin ensin teoriapohjaista ratkaisua. Toimeksiantajalla on kuitenkin paljon teoreettista tietämystä aiheesta jo valmiiksi, joten käytännöllinen ratkaisu todettiin hyödyllisemmäksi. Tutkimusongelman

ratkaisussa pyritään siis hyödyntämään Xamkin tarjoamia testiympäristöjä. Testiympäristössä on mahdollisuus asentaa ja kokeilla ratkaisuun sopivia työkaluja.

Primäärin aineiston keruumenetelmät ovat kokeilu, testaus ja kenttämuistiinpanot. Sekundääriaineistona toimii toimeksiantajan ja Microsoftin dokumentaatio sekä kaikki muu Windowsin tiedostojärjestelmiä käsittelevä dokumentaatio. Koska työ tähtää menetelmän muuttamiseen ja interventioon, jolla muutos saadaan aikaiseksi, työn lähestymistapa on interventionistinen kehittämistutkimus (Kananen 2017, 18).

3 TIEDOSTOJÄRJESTELMÄT

3.1 Tiedostopalvelin

Tiedostopalvelimen tarkoitus on toimia keskitettynä pisteenä tallennustilalle, johon samaan verkkoon liittyneet käyttäjät pääsevät käsiksi etänä. Tiedostopalvelimet ovat tärkeä osa yrityksen IT-infrastruktuurissa. Tallennustila keskitettynä yhteen pisteeseen helpottaa sen järjestelemistä ja konfiguraatiota ja turvaamista. Tiedostopalvelimet vaativat kuitenkin ylläpitoa, jonka takia nykypäivänä yritykset turvautuvat usein pilvipalvelujen varaan, mikä vähentää huomattavasti ylläpitotöitä. (Ingalls 2021.)

3.2 NTFS

NTFS on Windowsin käyttämä tiedostojärjestelmä, jonka mukana tulevat myös sen käyttökokemusta parantavat ominaisuudet. Se tukee esimerkiksi tiedostojen salausta ja pääsyn rajausta sekä ryhmä- että käyttäjätasolla. NTFS osaa myös hyödyntää lokitietoja tiedon palauttamiseen järjestelmävirheen jälkeen. (Microsoft 2021a.)

Morganin (2021) mukaan NTFS rajaa tiedostoihin pääsyä erilaisilla käyttöoikeuksilla, joita voi jakaa kansion eri tasoilla. Lista oikeuksista on seuraava:

- Full Control – kattaa kaikki NTFS-oikeudet, joiden lisäksi käyttäjä voi muokata toisten käyttäjien oikeuksia Full Control -oikeus mukaan lukien
- Modify – oikeus muokata, luoda ja poistaa tiedostoja sekä ominaisuuksia
- Read and execute – oikeus lukea ja suorittaa tiedostoja

- List folder contents – oikeus nähdä alikansiot ja nähdä sekä suorittaa tiedostoja
- Read – oikeus nähdä tiedostot ja kansiot, niiden ominaisuudet, sekä lukea tiedostojen sisältöä
- Write – oikeus kirjoittaa tiedostoon, lisätä tiedostoja kansioon ja lukea tiedostoja

Alikansiot ja tiedostot voivat periä NTFS-käyttöoikeuksia yläkansioilta, mikäli käyttöoikeuksien perintä on kytketty päälle alikansion tai tiedoston ominaisuuksissa. Alikansio tai tiedosto hakee oikeuksia ketjuna yläkansioistaan niin kauan, kunnes se kohtaa kansion, jossa käyttöoikeuksien perintä on kytketty pois päältä. (Sys-Manage 2021.)

3.3 Tiedostojaot

Windowsin jaetuissa kansioissa on myös omat käyttöoikeutensa, jotka ovat käytössä samanaikaisesti NTFS-käyttöoikeuksien kanssa. Morgan (2021) huomioi, että niin sanotut jaetun resurssin käyttöoikeudet ovat paljon suppeammat:

- Read – oikeus nähdä tai lukea tiedostoja, kansioita, ja ominaisuuksia
- Change – read-oikeus, sekä oikeus muokata, luoda, ja poistaa tiedostoja ja kansioita
- Full Control – samanlainen, kuin NTFS Full Control

Jaetun resurssin käyttöoikeudet pätevät koko jaettuun kansioon, eikä niitä voi säädellä alemmalla tasolla esimerkiksi alikansioissa.

Tiedostoa tai kansiota käsitellessä Windows tarkistaa sekä jaetun resurssin käyttöoikeudet että NTFS-käyttöoikeudet. Käyttäjän molempia käyttöoikeuksia vertaillaan ja molemmista listoista rajoitetuimmat oikeudet otetaan käyttöön. (Sys-Manage 2021.)

3.4 Haavoittuvaisen tiedostonjakoympäristön vaarat

Tietovuoto yrityksessä voi tapahtua sisä- ja ulkopuolelta. Työntekijä yrityksessä voi levittää arkaluontoista tietoa pelkästään vahingonilon takia, mutta hän voi myös tavoitella rahallista voittoa. Yrityksen ulkopuolelta rikolliset voivat päästä käsiksi arkaluontoiseen tietoon monella eri tapaa. Yksi tavoista on käyttäjätunnuksien varastaminen työntekijältä. Tämä onnistuu esimerkiksi tietojenkalastelulla tai brute force -hyökkäyksellä. (Kaspersky s.a.)

Arkaluontoisen tiedon levitessä yritys voi kärsiä monella eri tapaa. Yrityskustannuksia syntyy muun muassa toimintahäiriöistä, kyberturvallisuustutkinnoista ja mahdollisista oikeudenkäynneistä. Tietenkin myös yrityksen maine kärsii, mikäli tieto tietoturvaloukkauksesta leviää julkisuuteen. (Imperva s.a.)

4 TIEDOSTOJÄRJESTELMIEN SUOJAUSTA AJAVAT PROSESSIT

4.1 File Audit

Windowsin ominaisuus *Security auditing* mahdollistaa erilaisten tietoturvaan liittyvien tapahtumien nauhoittamisen. Nauhoituksen tarkoituksena on tallentaa lokeihin onnistuneita ja epäonnistuneita hyökkäyksiä tärkeisiin resursseihin. (Microsoft 2021b.)

Asetuksista voi määrittää monitoroinnin erityyppisille kategorioille. Näistä yksi on ”*Audit object access*”, joka nauhoittaa onnistuneet ja/tai epäonnistuneet yritykset käyttää käyttöoikeuksia. Kun tämä kategoria on konfiguroitu, järjestelmänvalvoja voi määrittää kansiot ja tiedostot, joita hän haluaa valvoa. Lokitiedot käyttöoikeuksien käytöstä tallentuvat turvalokiin, jota voi myöhemmin tutkia. (Microsoft 2021c.)

4.2 Data Loss Prevention

Data Loss Prevention (DLP) käytäntönä pyrkii estämään käyttäjiä levittämästä arkaluontoista informaatiota vääriin käsiin. Tiedostopalvelinten kontekstissa DLP on esimerkiksi ohjelmisto, joka skannaa tiedostojärjestelmiä tietyin väliajoin ja etsii arkaluontoiseksi luokiteltua sisältöä. DLP-työkalut voidaan konfiguroida hälyttämään erilaisista tunnisteista, kuten:

- Tietyn muotoiset ja kokoiset merkkisarjat, jotka muistuttavat esimerkiksi sosiaalitunnuksia tai pankkikortin tietoja
- Suora vertaus määritettyyn tietokantaan
- Tiedoston sormenjäljen vertaus

Skannauskriteerejä voi yleensä määrittää alusta loppuun itse tai hankkia kolmannelta osapuolelta alustavia kategorioita muokattavaksi. (Trellix s.a.)

Kun arkaluontoista informaatiota löytyy, Microsoftin (2022) tarjoamilla esimerkeillä DLP-työkalu voi muun muassa:

- Estää/varoittaa käyttäjää siirtämästä tiedostoa
- Siirtää arkaluontoisen tiedoston karanteeniin erikseen määritettyyn kansioon
- Lähettää järjestelmänvalvojalle hälytyksen

4.3 Identity Access Management

Identity Access Management (IAM) tarkoittaa toimintaperiaatetta, jota noudattamalla käyttäjät pääsevät käsiksi juuri heille kuuluviin resursseihin juuri silloin kun niille on tarvetta. IAM-järjestelmät auttavat järjestelmänvalvojia hallitsemaan käyttäjien sisäänkirjautumisia ja resurssien käyttöoikeuksia. Koska IAM toimii yrityksen tärkeiden resurssien ja käyttäjien välissä, sillä on tärkeä rooli kaapattujen käyttäjätilien hyväksikäytön torjunnassa. (IBM s.a.)

IAM tukee vahvasti vähimpien oikeuksien periaatetta ja pyrkii jakamaan käyttöoikeuksia tasaisesti käyttäjille niin, ettei vastuu jokaisesta IT-ympäristön osasta päädy vain yhdelle henkilölle. IAM täyttää yrityksen tietoturvavaatimuksia ja sen teknologioita ja työkaluja on suunniteltu kaiken kokoisille yrityksille. (Gittlen & Rosencrance s.a.)

Vähimpien oikeuksien periaate pyrkii ympäristöön, missä käyttäjillä, ohjelmilla ja prosesseilla on pienin mahdollinen määrä käyttöoikeuksia tarpeellisten tehtävien suorittamiseen. Haittaohjelmat hyödyntävät käyttöoikeuksia, joilla kyseinen ohjelma käynnistetään. Tämä tarkoittaa, että rajatuilla käyttöoikeuksilla myös haittaohjelman mahdollisuudet tuottaa vahinkoa ympäristöön ovat rajoittuneet. (CyberArk s.a.)

5 NYKYTILANTEEN KATSAUS

Toimeksiantaja on käynyt vuosien varrella läpi IT-infrastruktuurin muutoksia. Vanhasta infrastruktuurista on jäänyt jälkiä nykyisiin konfiguraatioihin. Esimerkiksi käyttäjäryhmillä on edelleen vanhojen nimeämiskäytäntöjen mukaisia nimiä, jotka eivät enää nykypäivänä päde.

Suomen paikallista IT-tiimiä haastatellessa ilmenivät seuraavat asiat:

- Käyttäjäryhmien liiallisen määrän kanssa on ollut ongelmia. Käyttäjät ovat kuuluneet liian moneen ryhmään, mikä on tuonut toimintahäiriöitä käyttöoikeuksiin.

- Tähän mennessä ei ole käyttöönotettu työkaluja, joilla monitoroidaan tiedostojen muokkausta tai poistoa.
- Tiedostojärjestelmistä ei myöskään säännöllisesti skannata arkaluontoista informaatiota.
- Paikallinen IT osoitti kiinnostusta IAM- ja DLP-menetelmille.

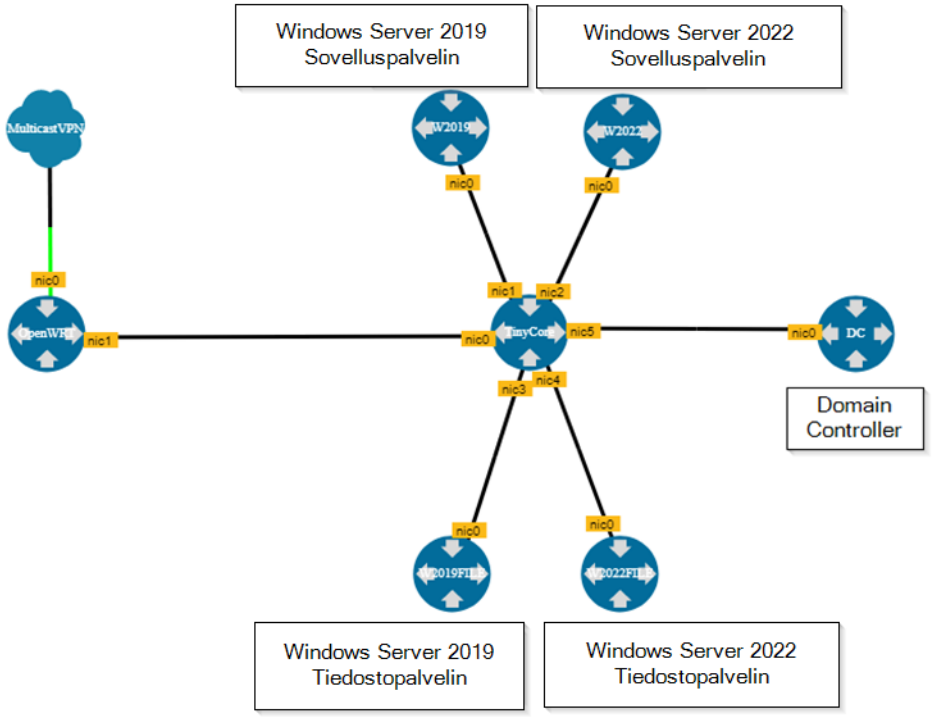
Client-tiimi puolestaan osoitti haastattelussa kiinnostusta yleisille käytännöille tiedostojärjestelmien hallintaan.

On myös hyvä huomioida, että toimeksiantaja käyttää monipuolisesti erityyppisiä tiedostonjakopalveluja. Tämä työ keskittyy kuitenkin kehittämään Windows-tiedostopalvelimia.

6 TUTKITUT KÄYTÄNNÖT JA RATKAISUT

Työn aikana ei tehdä muutoksia toimeksiantajan ympäristöön. Sen sijaan työssä testataan eri ratkaisuja Xamkin virtuaalisessa laboratoriossa.

Kaikki virtuaaliympäristöä tarvitsevat testit toteutetaan valmiiksi luodussa testiympäristössä (kuva 1). Testiympäristössä on viisi Windows Server -palvelinta. Kaksi palvelinta (Windows Server 2019 ja Windows Server 2022) toimii tiedostopalvelimina, kaksi palvelinta (Windows Server 2019 ja Windows Server 2022) toimii sovellusten hallintapalvelimina ja viides palvelin toimii Domain Controllerina. Ympäristön toimialueeseen “kissa.local” on lisätty testikäyttäjiä sekä testikäyttäjäryhmiä. Palvelimet kykenevät kommunikoimaan keskenään, ja ympäristössä toimii yhteys internetiin.



Kuva 1. Testiympäristön topologia

Tavoitteena oli löytää toimeksiantajalle ehdotettavia sopivia työkaluja ja periaatteita, jotka auttaisivat haastatteluissa ilmenneisiin ongelmiin.

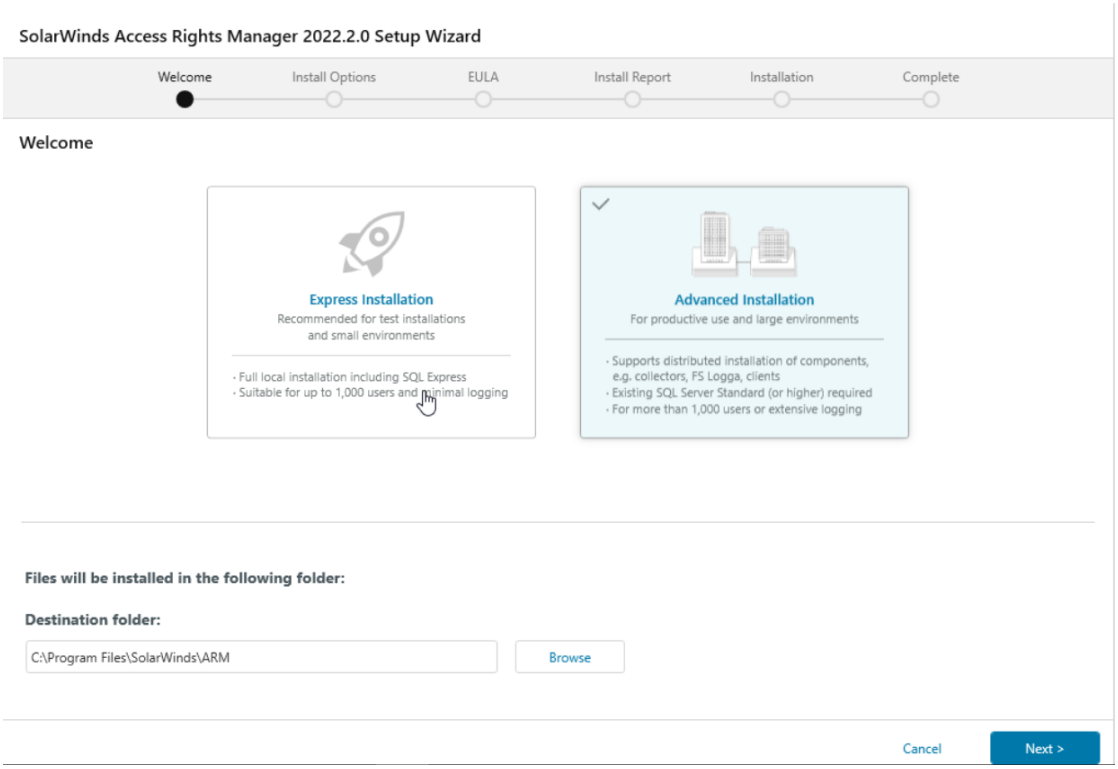
6.1 IAM-työkalu

IAM-työkalut tarjoavat vaihtelevasti eri palveluja. Toimeksiantajan tarpeita ajatellen niistä tärkein on kuitenkin kyky monitoroida ja hallita käyttäjien käyttöoikeuksia. SolarWindsin Access Rights Manager (ARM) -työkalun tarjoamia ominaisuuksia tutkittaessa ilmenee heti, että se helpottaa käyttöoikeuksien tutkimista ja monitorointia. SolarWinds tarjoaa myös kuukauden kestävän kokeilulisenssin työkaluaan varten. Kyseinen työkalu sisältää myös DLP-komponentteja.

6.1.1 SolarWinds ARM:n asennus ja käyttöönotto

Jotta työkalua päästään testaamaan, se ladataan ja asennetaan ensin testiympäristöön. Sovelluspalvelimeen (Windows Server 2019) asennetaan työkalun konfigurointi- ja hallintasovellukset. Ennen asennuksen etenemistä ARM vaatii Microsoft .NET Frameworkin asennuksen.

Asennuksen alussa vaihtoehtona on Express Installation ja Advanced Installation (kuva 2), joista ensimmäistä suositellaan testailua varten. Express Installation on myös rajattu tuhanteen käyttäjään, mitä testiympäristö ei ylitä. Express Installation sisältää oman SQL-asennuksen, joka edelleen helpottaa testausta.



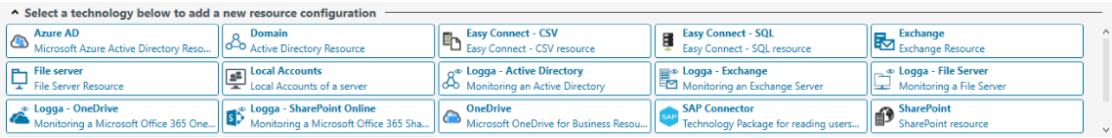
Kuva 2. Solarwinds ARM asennusvaihtoehdot

Ensimmäinen yritys asennuksessa epäonnistui liian vähäisen muistin takia. Muistia on kuitenkin helppo lisätä Xamkin virtuaalilaboratoriossa, joten ongelman saa korjattua parissa minuutissa. Muistin määrä muutetaan kolmesta gigatavusta vaadittuun kahdeksaan gigatavuun. Toisella yrityksellä asennus ei tuota ongelmia.

Ensimmäisellä sisäänkirjautumisella täytyy käyttää asennuksen aikana käytettyä Windows-tiliä, mutta käyttäjiä voi lisätä jälkikäteen. Työkalun ohjeistettu alustava konfigurointi voidaan suorittaa enimmäkseen oletusasetuksilla läpi valitsemalla:

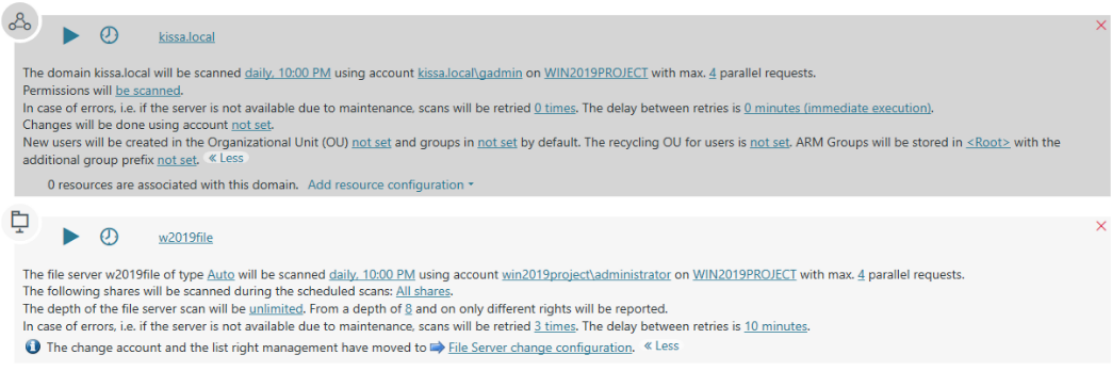
- Asennuksen aikana luotu SQL Server Instance
- Asennuksen aikana luotu tietokanta
- Testausta varten myönnetty sertifikaatti

Jotta Access Rights Managerin palveluja päästään testaamaan, sen konfiguraatiovalikon kautta täytyy vielä skannata yksi testiympäristön tiedostopalvelimista ja Active Directory (kuva 3).



Kuva 3. Konfiguraatiovalikko, josta skannataan “File server” ja “Domain”

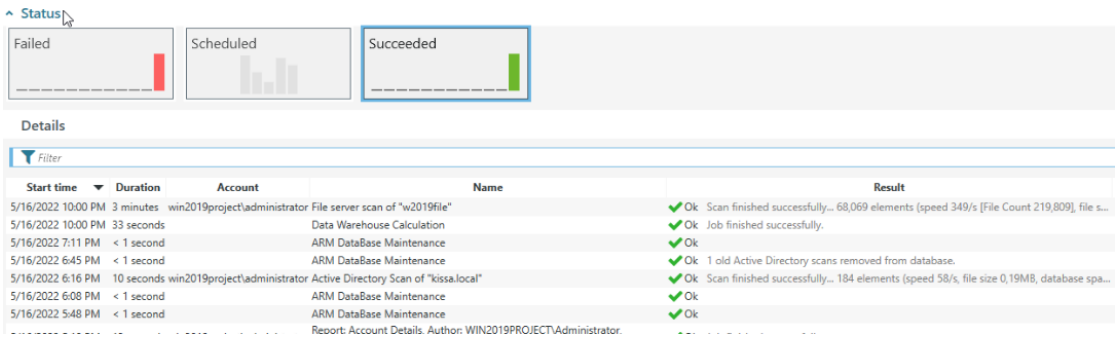
Kun tiedostopalvelin ja Active Directory on löydetty, niille voidaan määrittää eri asetuksia, kuten päivittäisiä skannauksia resurssien ajan tasalla pitämiseksi (kuva 4).



Kuva 4. Skannausasetukset testiympäristön toimialueelle (kissa.local) ja tiedostopalvelimelle (w2019file)

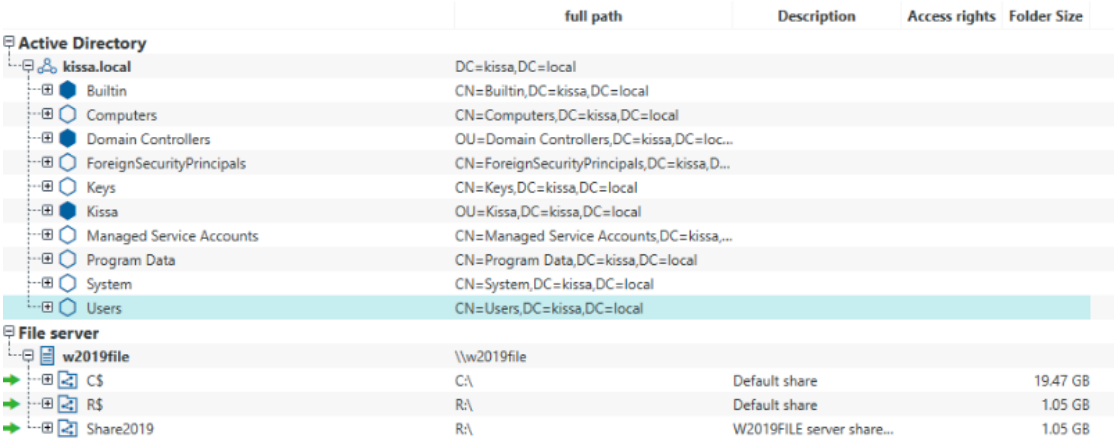
6.1.2 SolarWinds ARM:n toiminta

Onnistuneita (kuva 5) ja epäonnistuneita skannauksia voidaan tarkastella omasta osiostaan. Epäonnistuneista skannauksista näkee alustavan syyn epäonnistumiselle, mutta niistä voi myös avata lokitiedostot, joista saa tarkempaa tietoa. Vastaavasti onnistuneista skannauksista näkee alustavaa tietoa, kuten tiedostojen/objektien määrän.



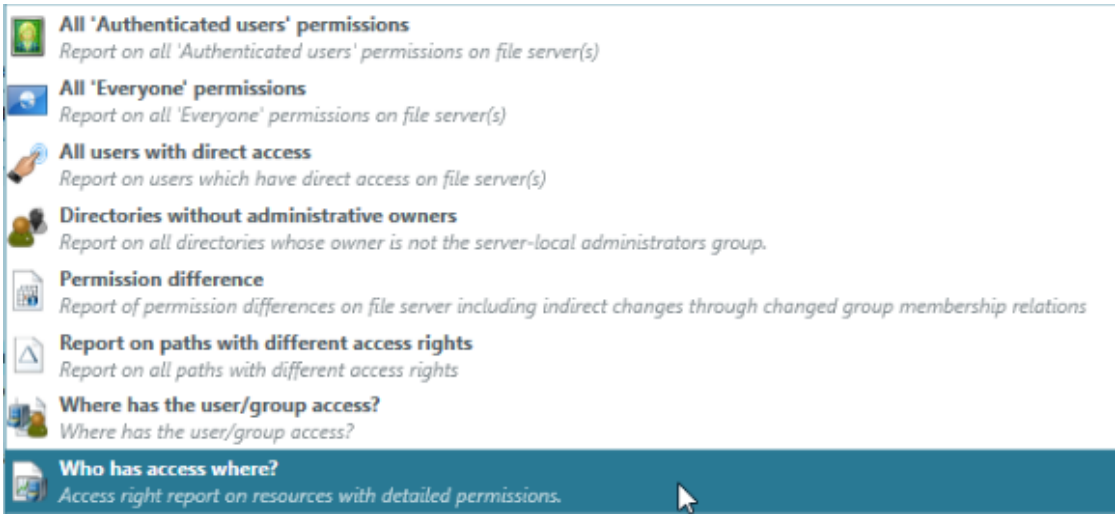
Kuva 5. Onnistuneet skannaukset

Resurssivälilehdestä löytää skannatun Active Directoryn ja tiedostopalvelimen (kuva 6). Näkymä on yksinkertainen ja siellä on helppo edetä poluissa syvemmälle.



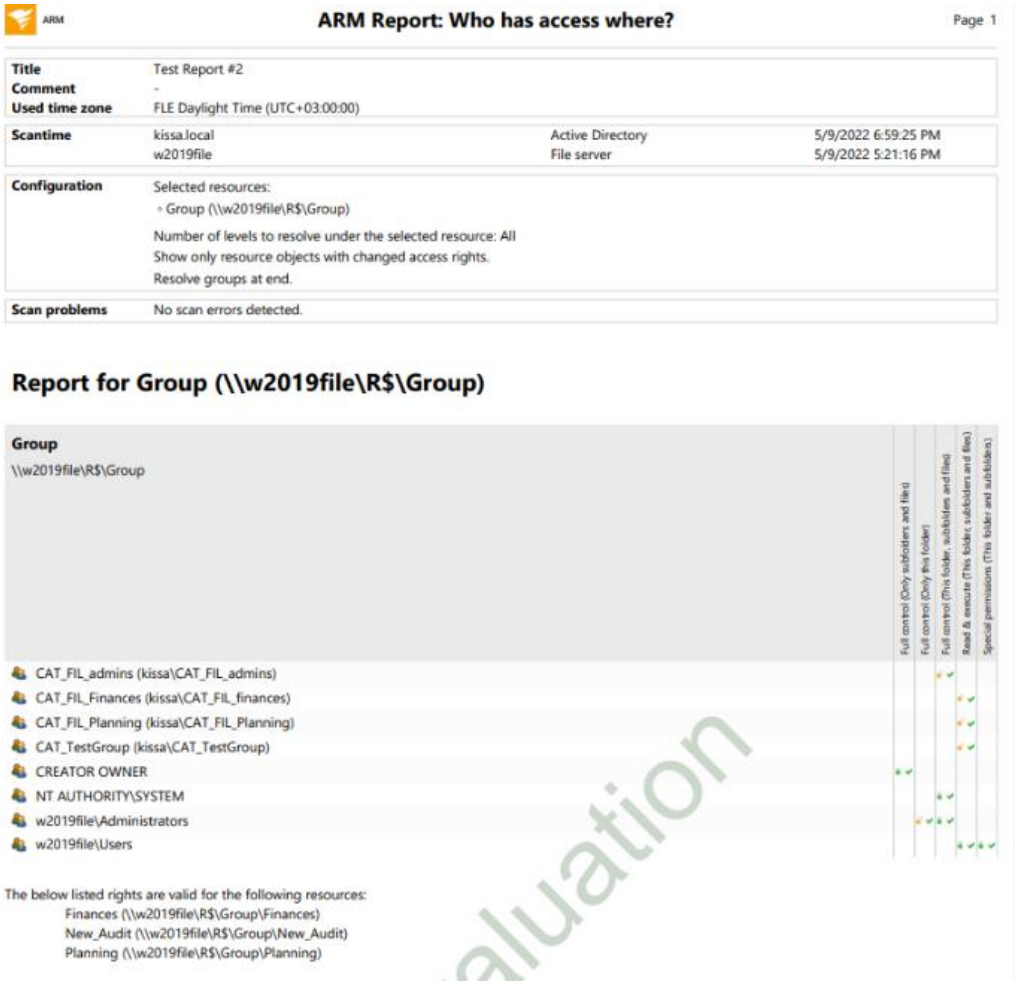
Kuva 6. Näkymä skannattujen resurssien sisällöille

Tiedostopalvelimen hakemistoista voi tuoda erimuotoisia raportteja kansiokohtaisesti (kuva 7). Kansiosta voi esimerkiksi tarkastaa nykyiset käyttöoikeudet tai muokkaushistorian kansion käyttöoikeuksiin.



Kuva 7. Vaihtoehdot raporteille

Nykyisistä käyttöoikeuksista ajetaan testinä raportti käyttämällä “Who has access where?” -raporttia. Kohteena on skannatusta tiedostopalvelimesta jaettu testikansio. Onnistuneen raportin ensimmäisistä tiedoista (kuva 8) näkee muun muassa raportille määritetyn nimen, resurssien viimeisimpien skannauksien päivämäärän, ja raporttia ajaessa ilmenneet virheet. Seuraava kohta näyttää, mitä käyttöoikeuksia milläkin käyttäjäryhmällä on kansiolle. Raportin lopussa (kuva 9) näkee vielä, mitä käyttäjiä aiemmin listattuihin käyttäjäryhmiin kuuluu.



ARM

ARM Report: Who has access where?

Page 1

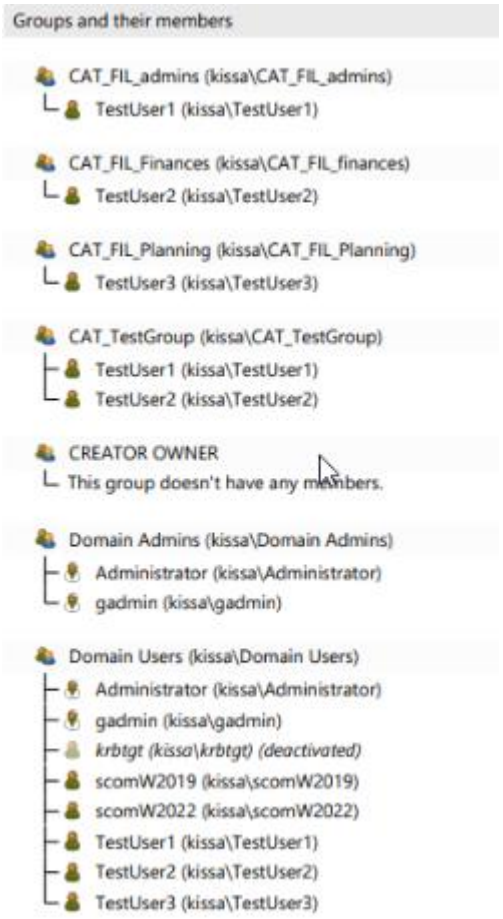
Title	Test Report #2		
Comment	-		
Used time zone	FLE Daylight Time (UTC+03:00:00)		
Scantime	kissa.local	Active Directory	5/9/2022 6:59:25 PM
	w2019file	File server	5/9/2022 5:21:16 PM
Configuration	Selected resources: ◦ Group (\\w2019file\R$\Group) Number of levels to resolve under the selected resource: All Show only resource objects with changed access rights. Resolve groups at end.		
Scan problems	No scan errors detected.		

Report for Group (\\w2019file\R$\Group)

Group \\w2019file\R$\Group	Full control (Only subfolders and files)	Full control (Only this folder)	Full control (This folder, subfolders and files)	Read & execute (This folder, subfolders and files)	Special permissions (This folder and subfolders)
CAT_FIL_admins (kissa\CAT_FIL_admins)			✓	✓	
CAT_FIL_Finances (kissa\CAT_FIL_finances)				✓	
CAT_FIL_Planning (kissa\CAT_FIL_Planning)				✓	
CAT_TestGroup (kissa\CAT_TestGroup)				✓	
CREATOR OWNER	✓				
NT AUTHORITY\SYSTEM			✓		
w2019file\Administrators		✓	✓		
w2019file\Users				✓	✓

The below listed rights are valid for the following resources:
Finances (\\w2019file\R$\Group\Finances)
New_Audit (\\w2019file\R$\Group\New_Audit)
Planning (\\w2019file\R$\Group\Planning)

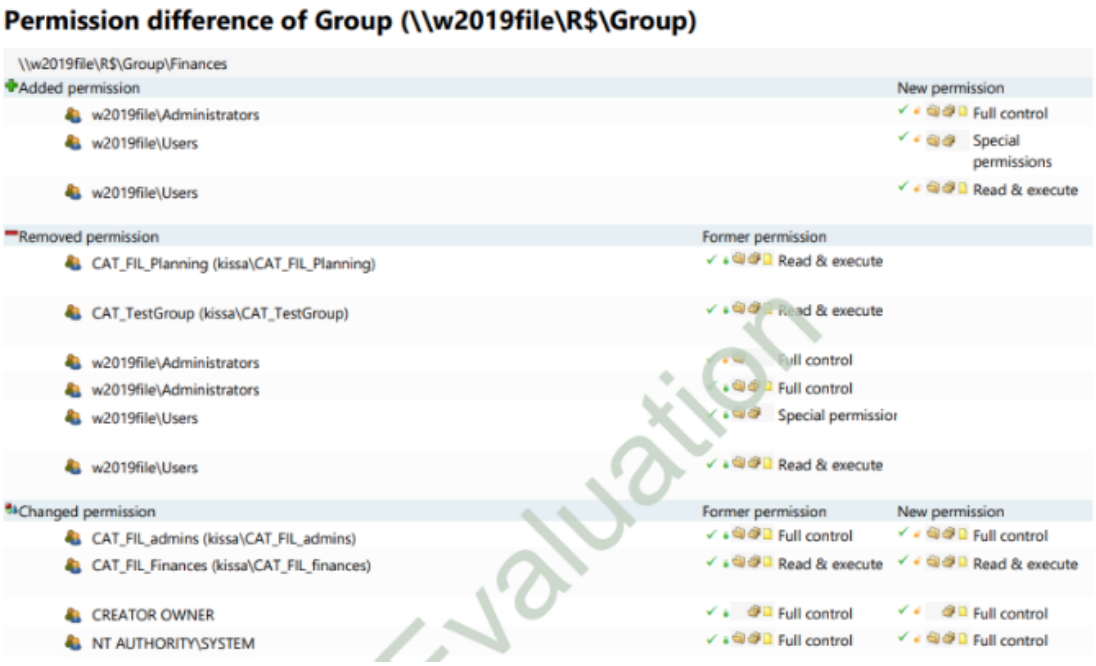
Kuva 8. Ensimmäinen osa raportista kansion nykyisistä käyttöoikeuksista



Kuva 9. Toinen osa ensimmäisestä testiraportista, josta näkee ryhmien jäsenet

Tiedostopalvelimesta ajetaan vielä toinen testi. Vaihtoehdolla “Permission difference” haetaan raportti, joka näyttää muokkaushistorian kansion käyttöoikeuksille. Asetuksiin lisätään myös, että raportti näyttää muokkaukset alikansioihin ja asetetaan ajankohdaksi muokkaukset viimeisimmältä vuodelta.

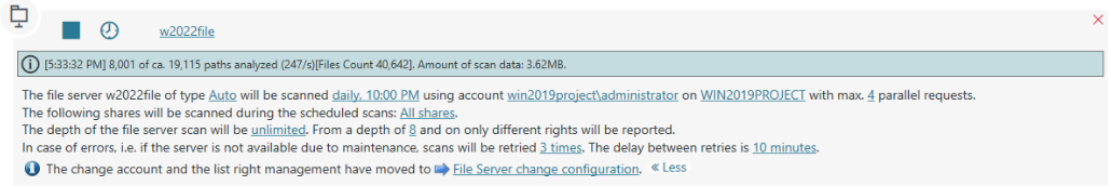
Onnistuneesta raportista näkee nyt muutokset käyttöoikeuksiin alikansiokohtaisesti. Kuvasta 10 näkee kolmeen kategoriaan jaetut muutokset, jotka ovat lisätyt oikeudet, poistetut oikeudet ja muutetut oikeudet. Raportin loppuosassa näkee epäsuoria muutoksia käyttäjien oikeuksiin, mitkä ovat aiheutuneet muutoksista käyttäjäryhmäjäsenyydessä. Esimerkiksi kuten kuvasta 11 näkee, käyttäjätili TestUser1 menetti Full control -käyttöoikeudet kansioon Group, koska se ei enää kuulu käyttäjäryhmään CAT_FIL_admins.



Kuva 10. Osa toisesta testiraportista

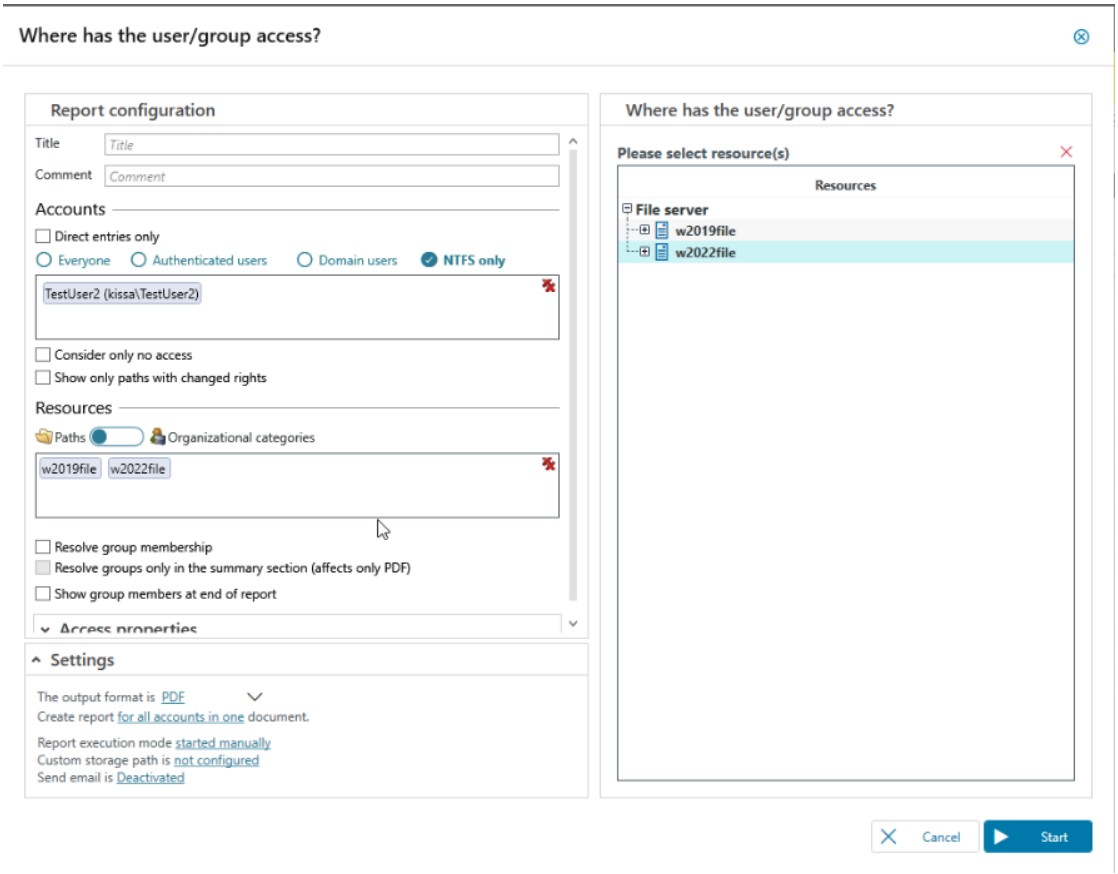
Kuva 11. Osa toisen testiraportin lopusta

Tähän mennessä kaikki raportit on tuotettu hyödyntämällä skannattua tiedostopalvelinta. Koska testitoimialue *kissa.local* on myös skannattu, testataan vielä sen resurssien raportointia. Toimialueen puolelta saadaan käyttäjäkohtaisia raportteja. Tätä varten skannataan uusi tiedostopalvelin testiympäristöstä, jotta saadaan parempia esimerkkejä testituloksiin.



Kuva 12. Toisen tiedostopalvelimen skannausasetukset

Onnistuneen skannauksen jälkeen Active Directory -resurssista etsitään testikäyttäjä ja tehdään testiraportti, joka näyttää käyttäjän käyttöoikeudet molemmissa tiedostopalvelimissa. Kuvassa 13 näkyy valittuna käyttäjä TestUser2 ja molemmat tiedostopalvelimet.

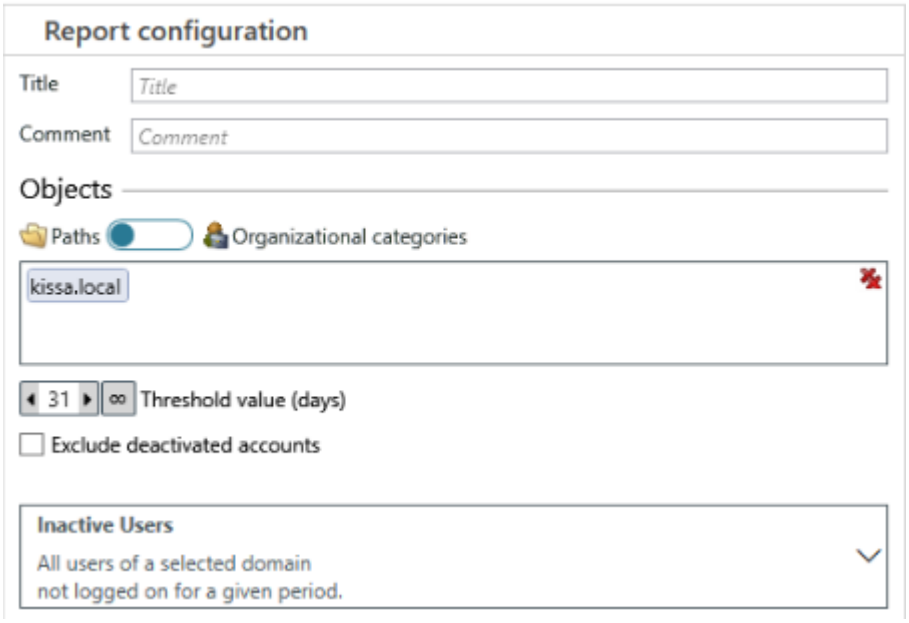


Kuva 13. Käyttäjän käyttöoikeusraportin asetukset

Onnistunut skannaus näyttää taas aluksi yleiset tiedot, jonka jälkeen se listaa käyttäjälle määritetyt oikeudet molemmissa tiedostopalvelimissa (kuva 14).

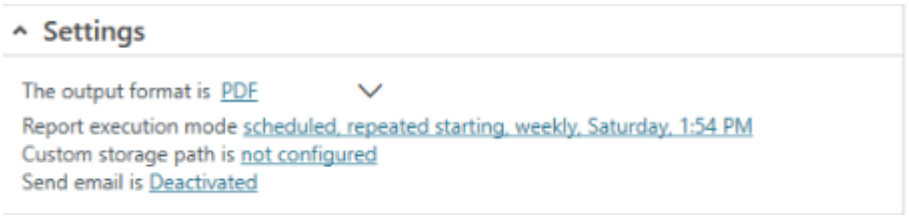
Kuva 14. Käyttäjän käyttöoikeusraportti

Toimialueesta voi laatia raportin käyttäjistä, jotka eivät ole kirjautuneet pitkään aikaan (kuva 15).



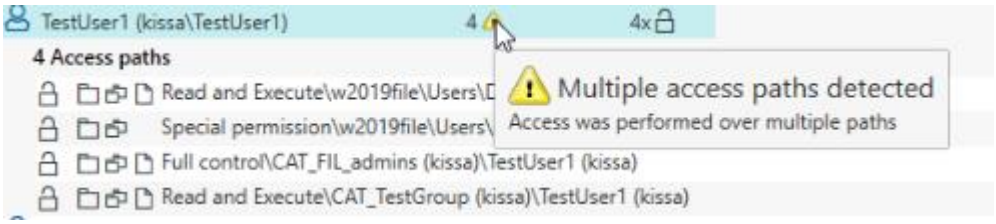
Kuva 15. Epäaktiivisten käyttäjien skannaus viimeisimmältä kuukaudelta

Kuten resurssien skannauksia, myös raportteja voidaan tuottaa automaattisesti esimerkiksi viikoittain (kuva 16). Raportit voidaan myös määrittää tulemaan käyttäjien sähköpostiin, jos SMTP-palvein on konfiguroitu.



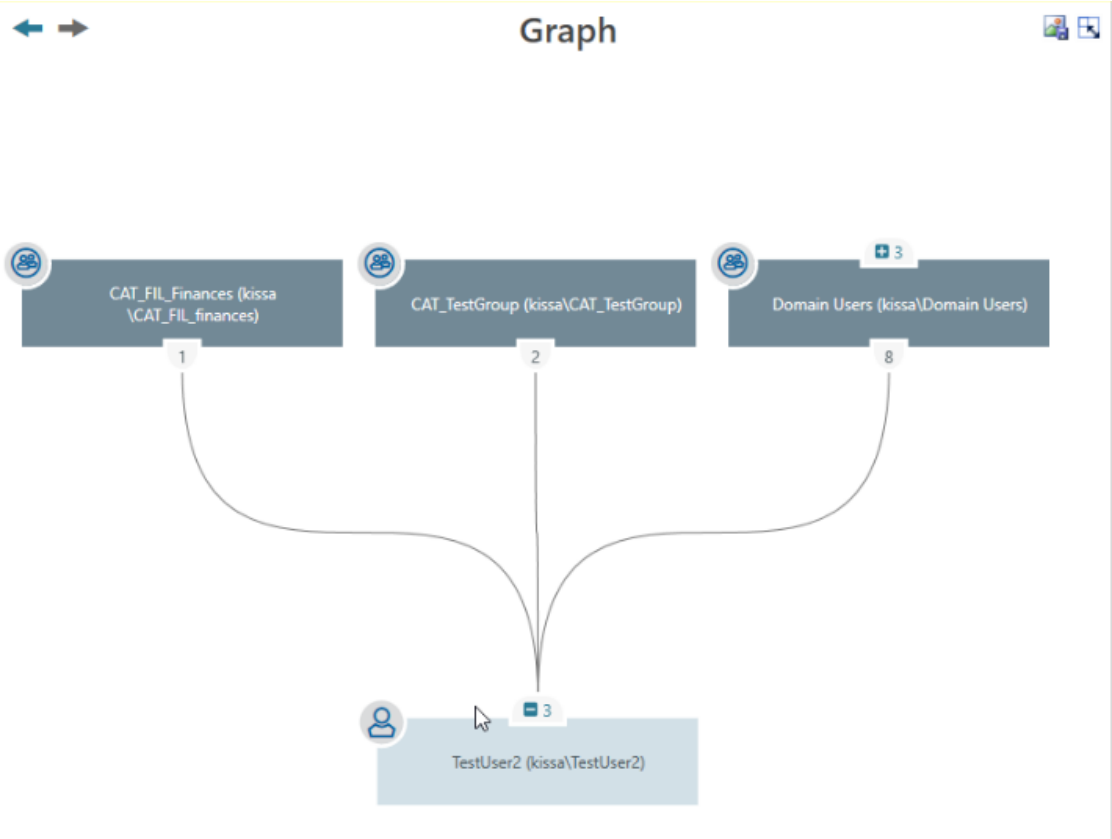
Kuva 16. Ajastetut raportit

Resurssivälilehdeltä voi valita kansion ja tutkia, kuinka paljon tiettyjen käyttäjien käyttäjäryhmät menevät päällekkäin käyttöoikeuksien kanssa (kuva 17). Tätä voisi tulkita tehokkaana työkaluna liiallisten käyttäjäryhmien karsimisessa, vaikkei se yksinään kyseistä ongelmaa pystykään ratkaisemaan.



Kuva 17. Testikäyttäjällä on sama käyttöoikeus kansioon neljästä eri ryhmästä

Käyttäjätilivälilehdestä on hyvä mainita sen verran, että kuten kuvasta 18 näkee, käyttäjiä ja niiden yhteyksiä käyttäjäryhmiin voi tutkia kaaviomuodossa, jossa voi liikkua vapaasti klikkailemalla käyttäjäryhmiä ja käyttäjiä.

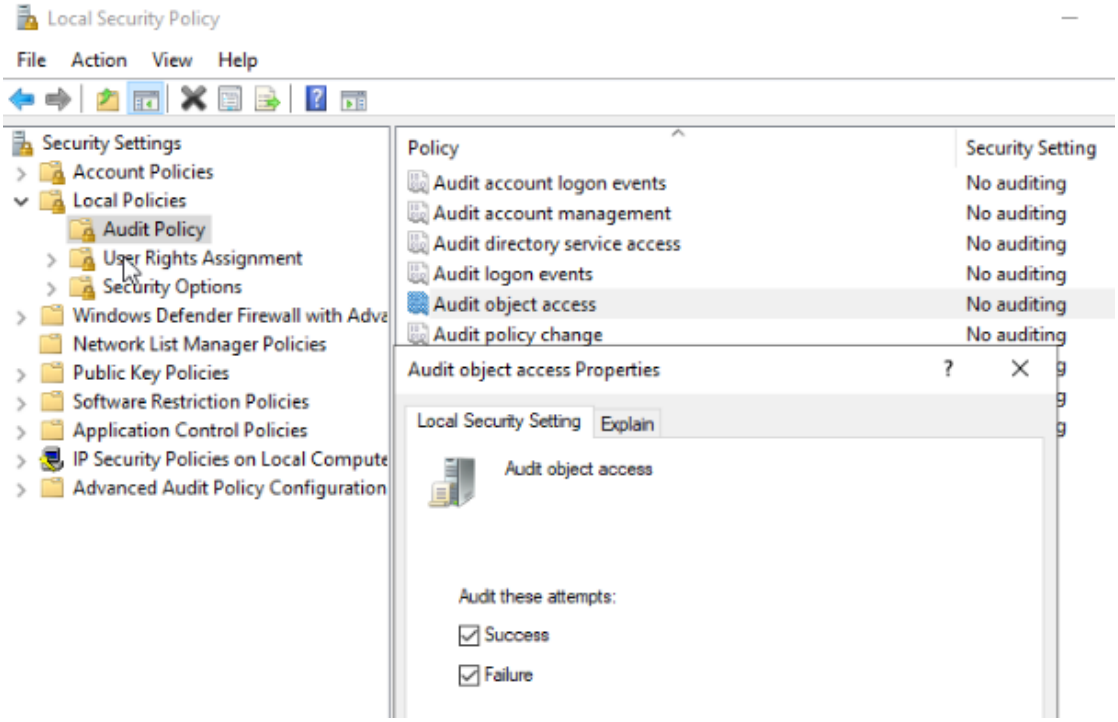


Kuva 18. Interaktiivinen kaavio käyttäjien ja käyttäjäryhmien välillä

6.2 Windows File Audit

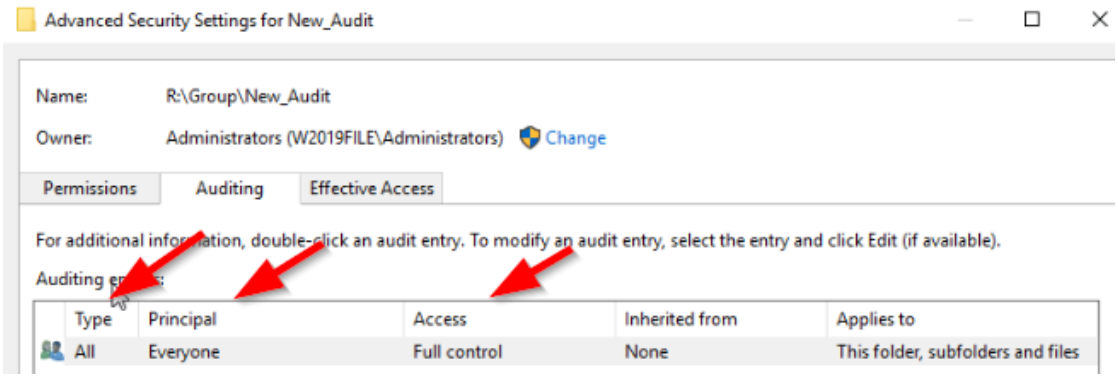
Windows File Auditin on tarkoitus toimia väliaikaisena ratkaisuna, sillä sen käyttöönotto on nopea ja helppo. Tiedostopalvelimeen konfiguroidaan auditointi, koska kuten aiemmin mainittu, se ei oletuksena ole Windows-laitteissa päällä.

Ensimmäinen vaihe on kytkeä tiedostopalvelimeen päälle *Audit object access*. Kuvasta 19 näkee, että asetuksen löytää Windowsin valikosta Local Security Policy. Tuplaklikkaamalla saadaan auki haetun policyn asetukset, josta kytketään päälle monitorointi sekä onnistuneille että epäonnistuneille yrityksille käyttää käyttöoikeuksia. Tämä asetus ei itsessään riitä lokien keräämiseen. Käyttäjän pitää määrittää itse ne kansiot, joita hän haluaa auditoida.



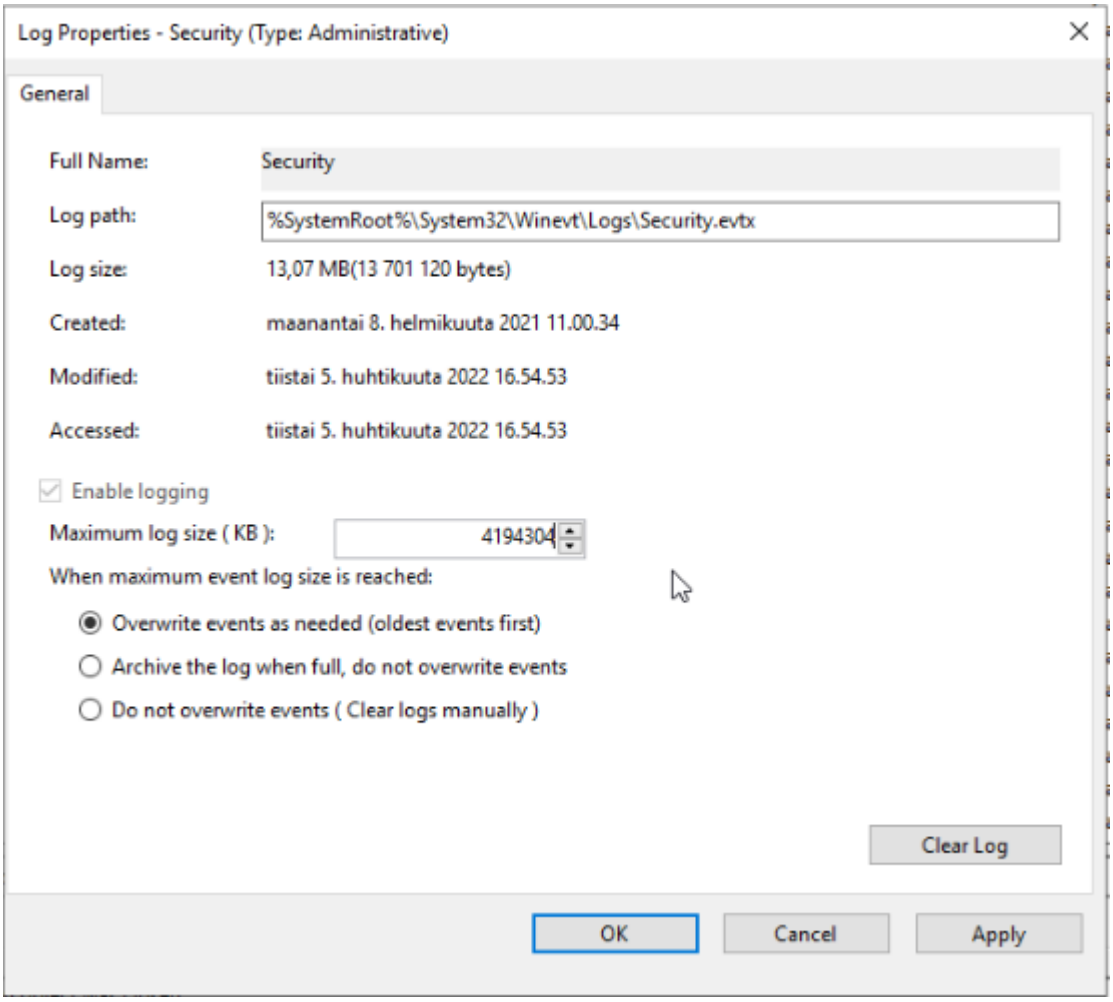
Kuva 19. Audit object access -policyn päälle kytkentä

Toisesta tiedostopalvelimen testikansiosta avataan asetukset. Asetuksista edetään *Security*-välilehdelle ja avataan lisäasetukset. Lisäasetuksista siirrytään vielä *Auditing*-välilehdelle, jossa päästään lisäämään käyttäjiä tai ryhmiä, joiden toiminnoista kansiossa halutaan kerätä lokeja. Asetukset määritetään kuvan 20 mukaan. Ensimmäinen nuoli osoittaa, että lokit kerätään sekä onnistuneista, että epäonnistuneista yrityksistä. Toinen nuoli osoittaa, että kaikkia käyttäjiä monitoroidaan. Viimeinen nuoli osoittaa, että kaikkia käyttöoikeuksia monitoroidaan.



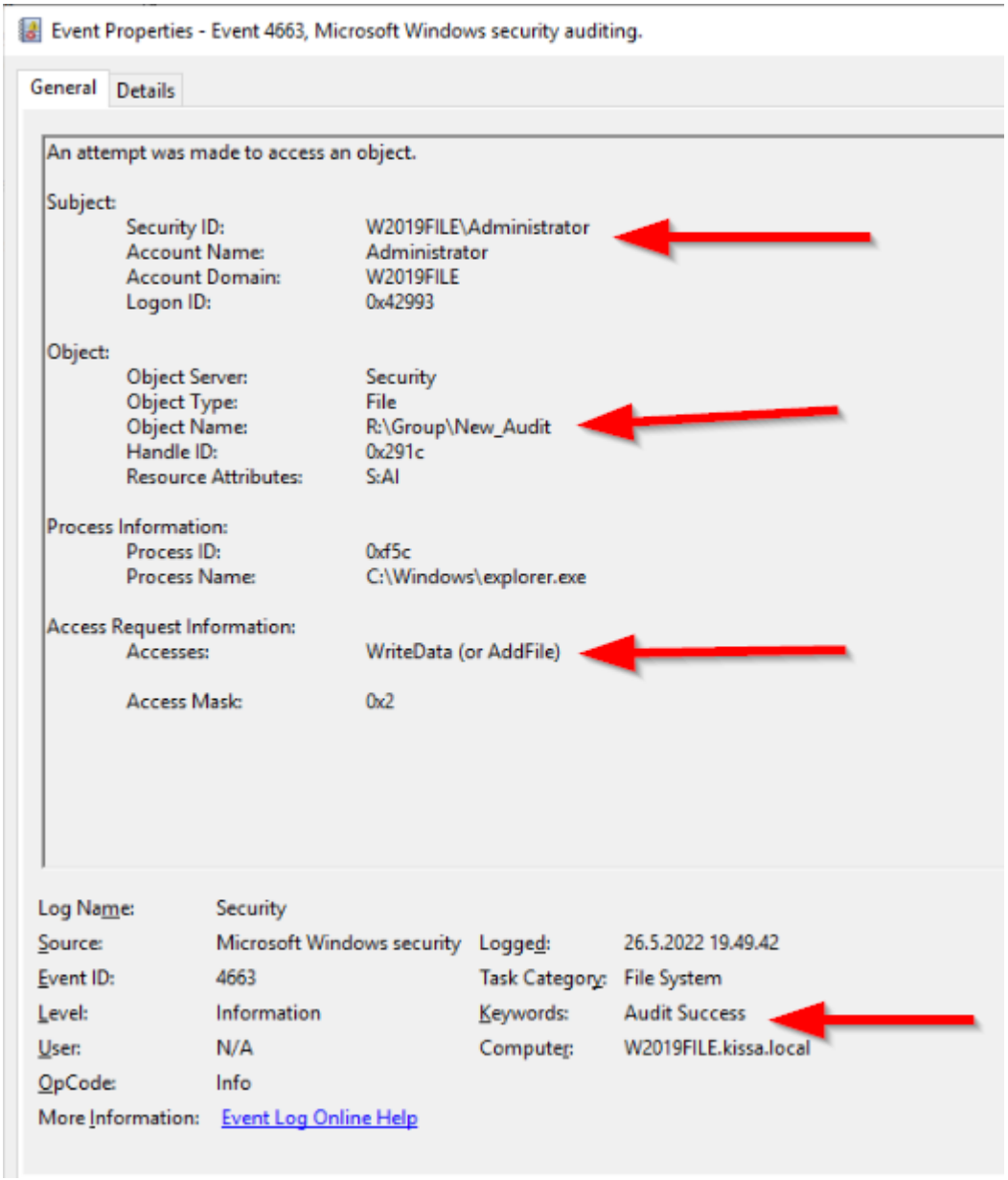
Kuva 20. Auditoitavan kansion asetukset

Seuraavaksi tiedostopalvelimesta avataan Windowsin Event Viewer ja vaihdetaan asetuksista turvalokien maksimikoko neljään gigatavuun. Määritetään myös, että tilan loppuessa uudet lokit korvaavat vanhat lokit. (Kuva 21.)



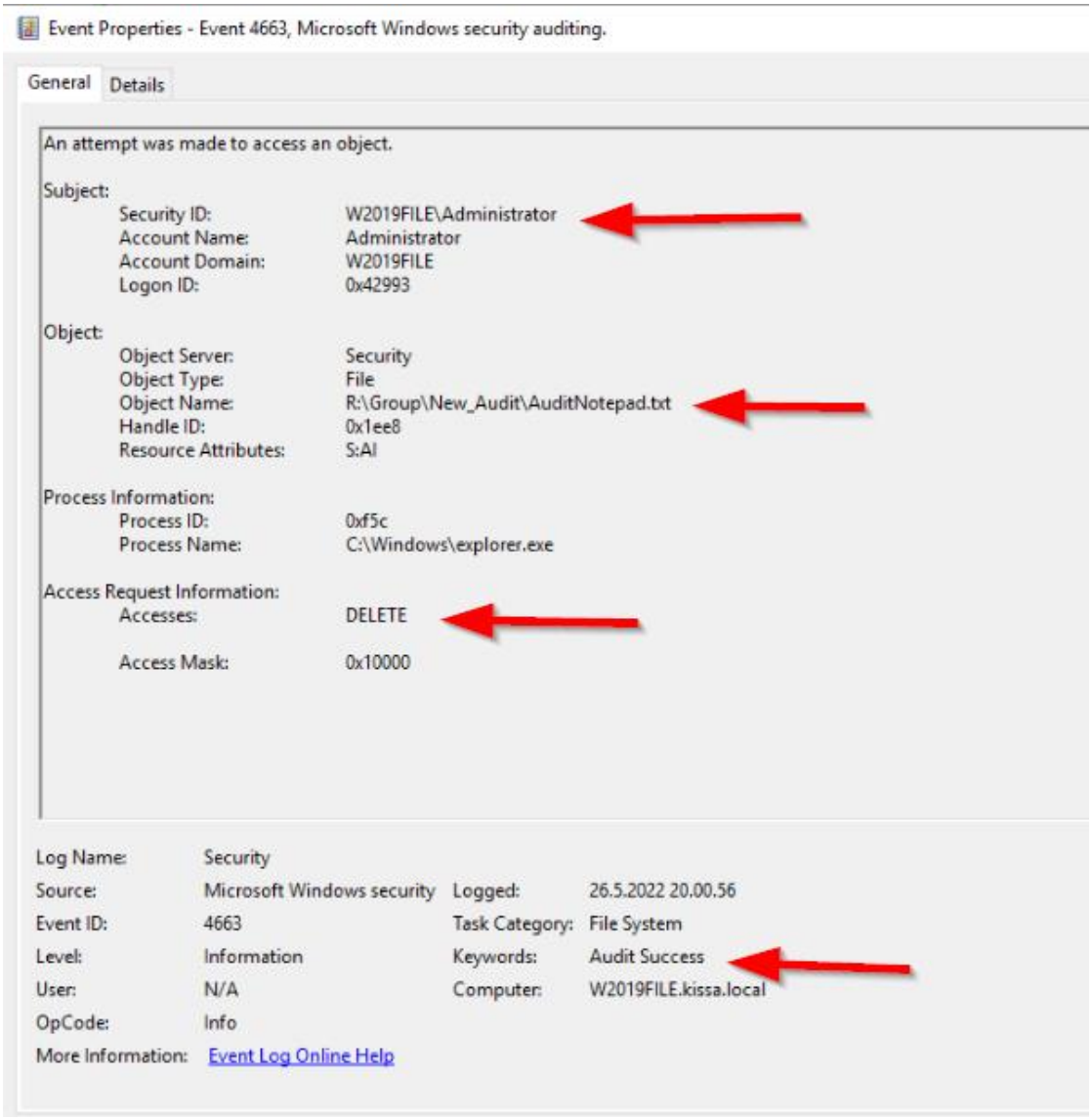
Kuva 21. Lokiasetukset

Jotta testituloksia saadaan tutkittavaksi, kohdekansioon tehdään pari tiedostoa ja myöhemmin niitä poistellaan. Tiedoston luonnin jälkeen yleisimmät tiedot lokilistasta löytää tunnisteella Event 4663. Kuvassa 22 on esimerkki lokista, jonka mukaan tiedostopalvelimen järjestelmänvalvoja on onnistuneesti luonut tai muokannut tiedostoa kansiossa R:\Group\New_Audit.



Kuva 22. Ensimmäinen esimerkkiloki

Kuvassa 23 on esimerkki lokista, jonka mukaan tiedostopalvelimen järjestelmänvalvoja on onnistuneesti poistanut aiemmin luodun tiedoston.



Kuva 23. Toinen esimerkkiloki

Windows File Auditin huono puoli on se, että jo pelkästään yhdestä tapahtumasta, esimerkiksi tiedoston luomisesta, jakaantuu tiedot moneen eri lokiin. Tästä syystä käyttäjien toimintaa on todella hankala monitoroida pelkästään Event Viewerin avulla.

6.3 DLP-työkalu

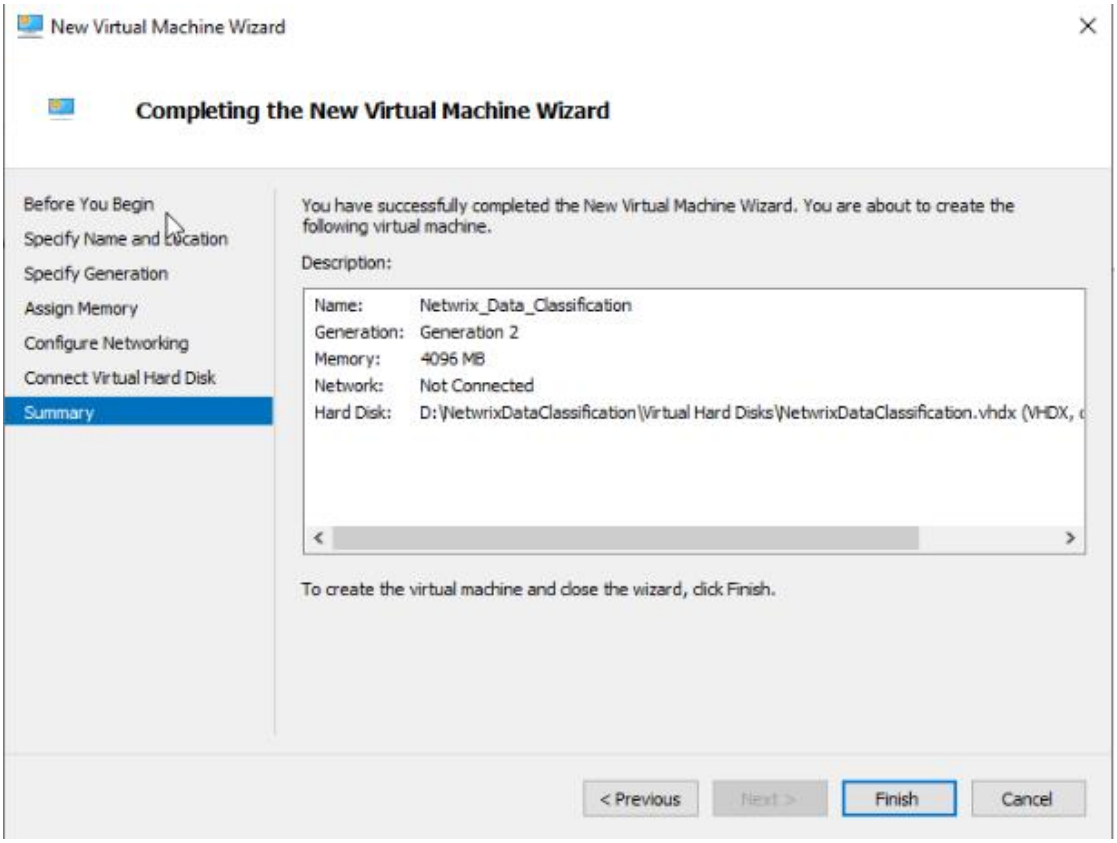
Netwrix Data Classification on arkaluontoista dataa etsivä ohjelma, jonka voi implementoida valvomaan esimerkiksi yrityksen verkkoa. Työkalun toiminta voidaan konfiguroida omien tarpeiden mukaan. Data Classification voi esimerkiksi klassifioida tiedostoja ja siirtää niitä karanteeniin. Data Classificationissa on valmiiksi määriteltyjä taksonomioita, joita voidaan käyttää arkaluontoisen

datan tunnistamiseen. Työkalun toimintaa voidaan myös automatisoida sen sisäisillä työnkuluilla. (Netwrix s.a.)

6.3.1 Netwrix Data Classificationin asennus ja käyttöönotto

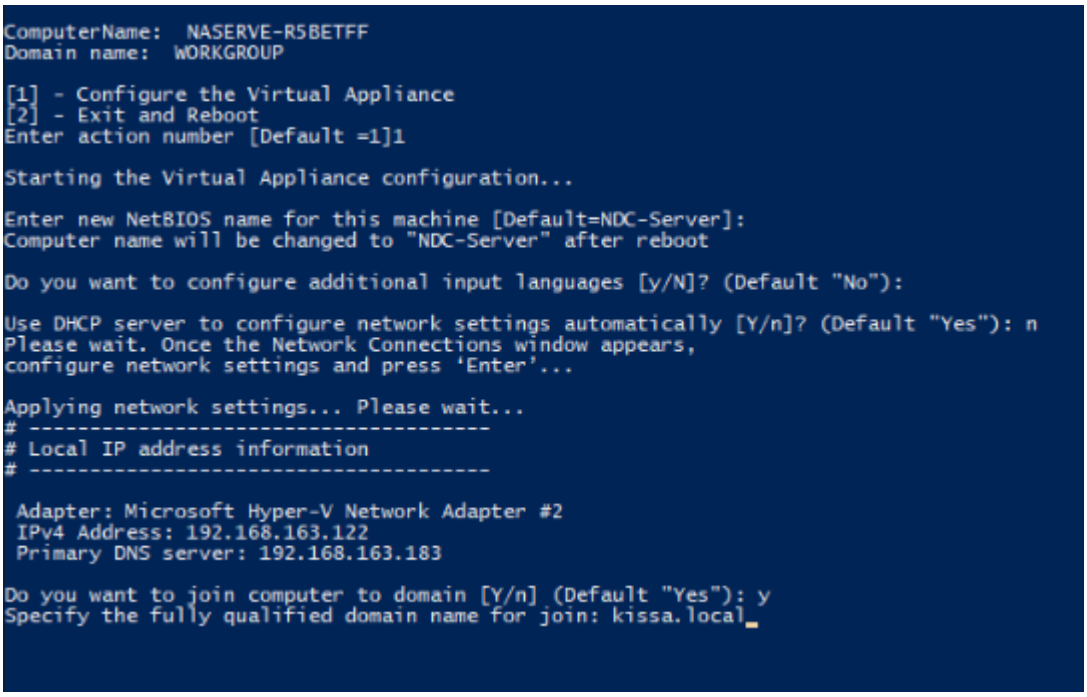
Netwrix Data Classification tarjoaa kokeiluversiota 20 päiväksi. Työkalu asennetaan Windows Server 2022 -sovelluspalvelimeen, jota ei tähän mennessä ole vielä hyödynnetty. Netwrixin verkkosivuilta voi ladata asennuspaketin ohjelmistolle, mikäli komponentit halutaan levittää omaan ympäristöön. Vaihtoehtoisesti Netwrixiltä voi myös ladata valmiin virtuaalisen kiintolevyn, johon on valmiiksi asennettu kaikki Data Classification -työkalun komponentit, mukaan lukien SQL-palvelin. Virtuaalisesta kiintolevystä voi myöhemmin luoda valmiin virtuaalikoneen. Tätä työtä varten ladataan valmis virtuaalinen kiintolevy, sillä sitä suositellaan varta vasten evaluointitarkoitukseen.

Windows Server 2022 -palvelimessa on valmiiksi asennettu Hyper-V, jonne Netwrixin virtuaalikone voidaan lisätä (kuva 24).



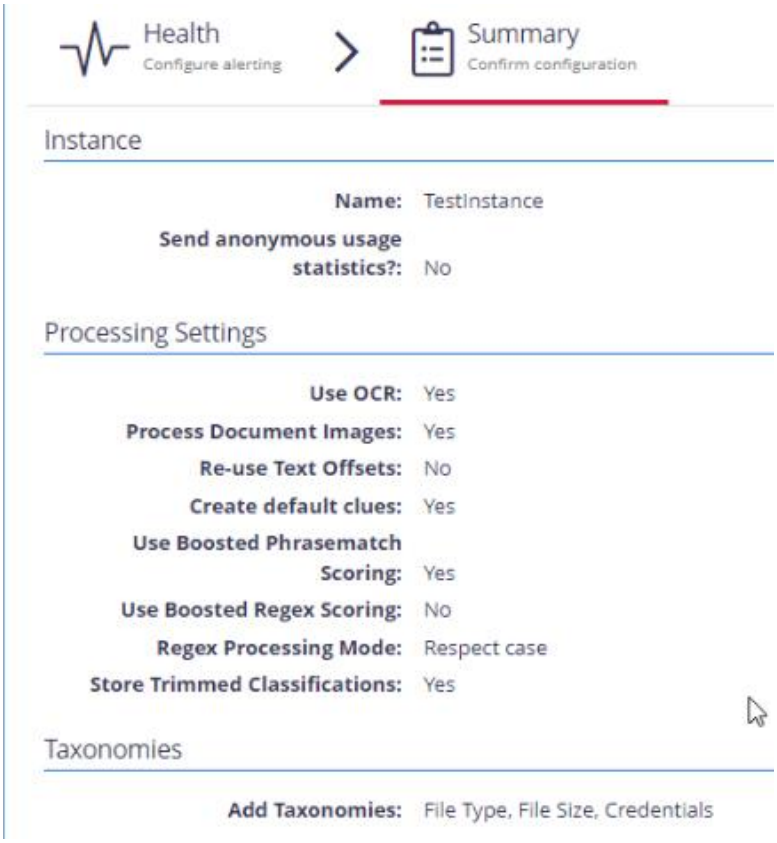
Kuva 24. Virtuaalikoneen luonti

Virtuaalikoneeseen asetetaan ensimmäisellä käynnistyksellä salasana ja alustavat konfiguroinnit. Konfigurointiin kuuluu laitteen nimi, kieliasetukset, verkkoasetukset ja toimialueeseen liittyminen (kuva 25).



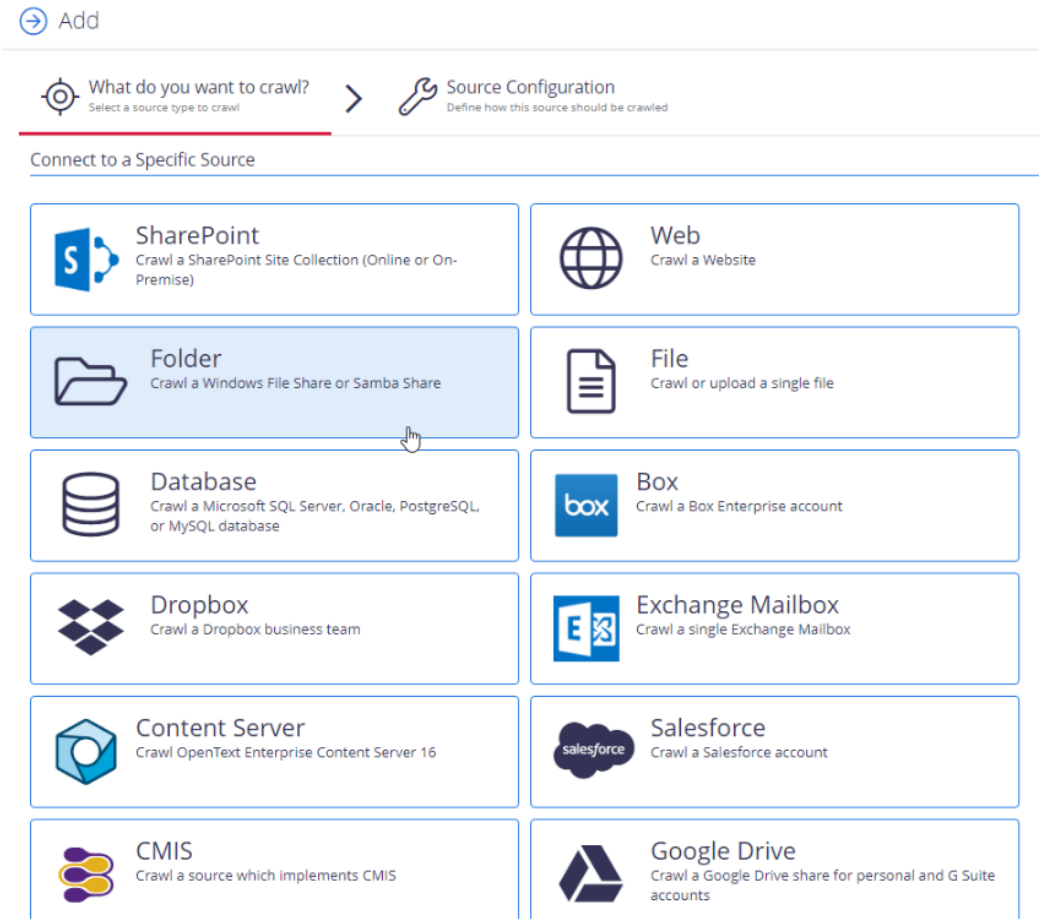
Kuva 25. Virtuaalikoneen konfigurointi

Asetuksien määrittäminen etenee seuraavaksi itse työkalun konfigurointiin. Työkaluun konfiguroidaan muun muassa tekstintunnistus kuvista, halutut taksonomiat tiedostojen skannauksia varten ja sallitut käyttäjät (kuva 26).



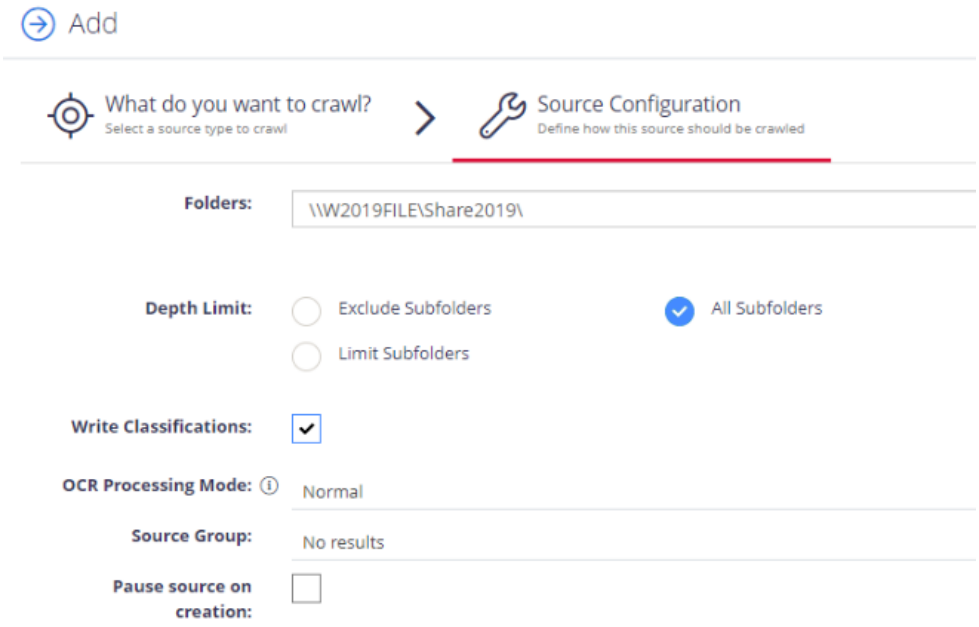
Kuva 26. Työkalun konfigurointi

Kun Netwrix Data Classification on konfiguroitu ja sitä ylläpitävä virtuaalikone on liitetty onnistuneesti testiympäristön toimialueeseen, työkaluun voidaan aloittaa skannattavien lähteiden lisääminen. Kuvasta 27 näkee, että Netwrix Data Classification mahdollistaa tiedostopalvelimien lisäksi myös monen muun lähteen skannaamisen, kuten Sharepointin ja sähköpostin, mistä voisi olla hyötyä toimeksiantajalle. Työ keskittyy kuitenkin tiedostopalvelimiin, joten muut lähteet unohdetaan tässä vaiheessa. Vaihtoehdoista valitaan Folder ja molempien tiedostopalvelimien jaetut kansiot lisätään lähteiksi.



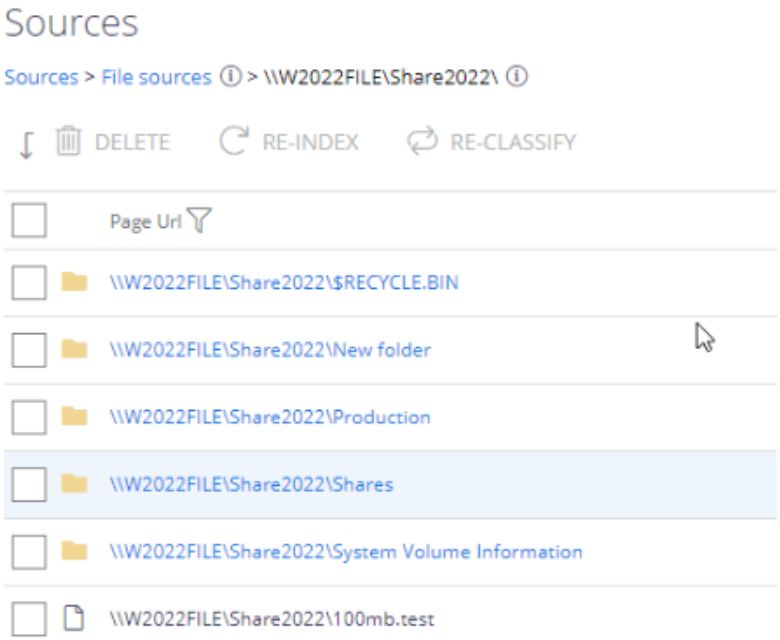
Kuva 27. Netwrix Data Classificationin vaihtoehdot skannattaville lähteille

Lähteen konfigurointiin asetetaan jaetun tiedoston polku ja tekstintunnistuksen tehokkuus (kuva 28). Tekstintunnistuksen tehokkuutta voidaan säätää, koska se vie enemmän resursseja, mitä tarkemmin se skannaa.



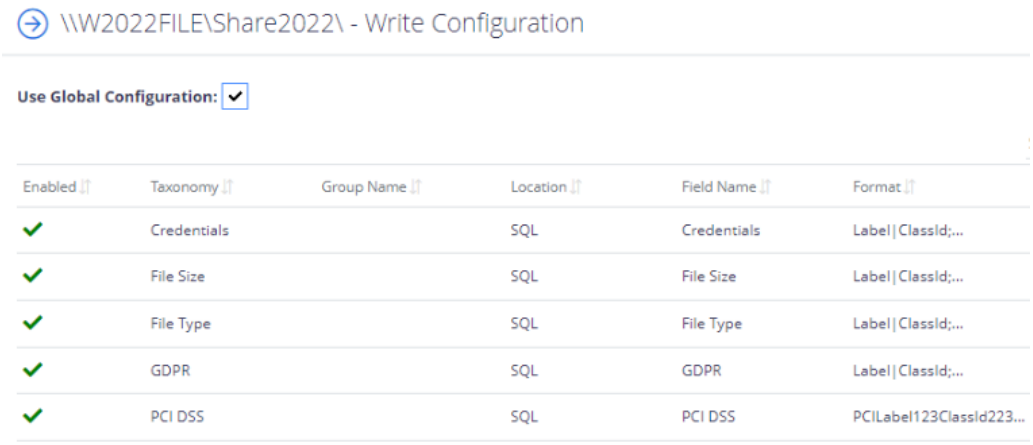
Kuva 28. Lähteen konfigurointi

Konfiguroinnin jälkeen työkalu tunnistaa jaetut kansiot. Kuvassa 29 näkyy esimerkkinä toisen kansion sisältö. Avatessa lähteen käyttäjä näkee kaikki tiedostot ja voi edetä kansiopolussa syvemmälle. Tiedostoista voidaan avata lisätietoja, ja mikäli taksonomiat on jo luotu ja asetettu lähteelle, tiedostojen klassifioinnit voidaan tarkistaa.



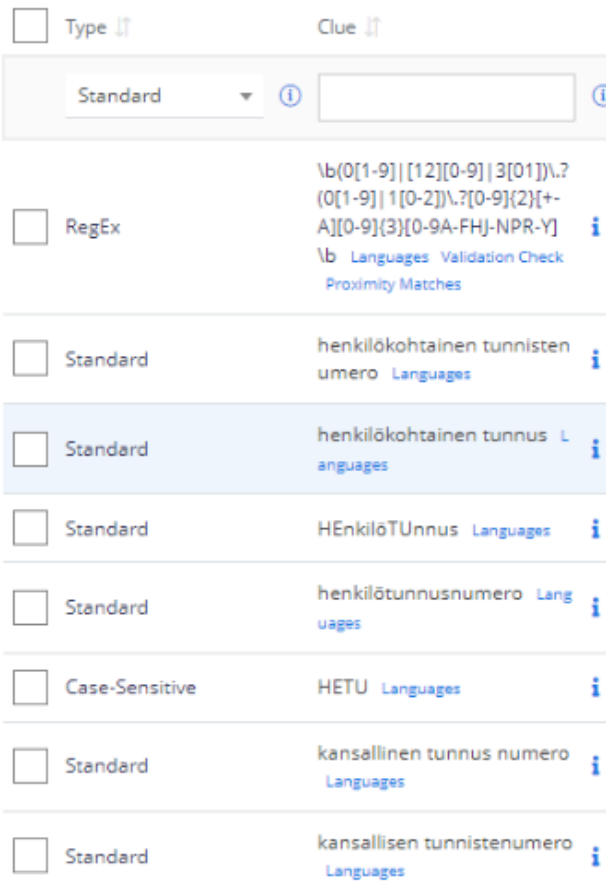
Kuva 29. Lähteen sisältö

Testattavia taksonomioita liitetään jaettuihin kansioihin (kuva 30). Netwrix on implementoinut valmiiksi yleisiä taksonomioita, kuten tietosuoja asetus General Data Protection Regulation (GDPR) ja maksukorttien tietosuojastandardi Payment Card Industry Data Security Standard (PCI DSS).



Kuva 30. Lähteisiin liitetyt taksonomiat

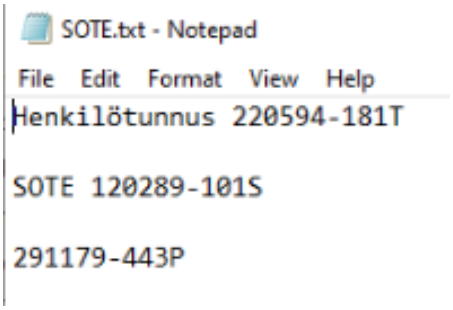
Netwrix Data Classificationin ylävalikosta voi avata listan taksonomioista, josta pääsee tutkimaan, mitä ne sisältävät. Esimerkiksi GDPR-taksonomia käyttää erilaisia henkilötietoihin liittyviä termejä tunnisteena (kuva 31). Termeihin on myös tarpeen mukaan asetettu ylimääräisiä sääntöjä, esimerkiksi isojen ja pienien kirjaimien pakollinen huomiointi. Oletustaksonomioiden tunnisteita ja niiden sääntöjä voi itse säätää tarpeen mukaan.



Kuva 31. GDPR-taksonomian tunnistamia termejä

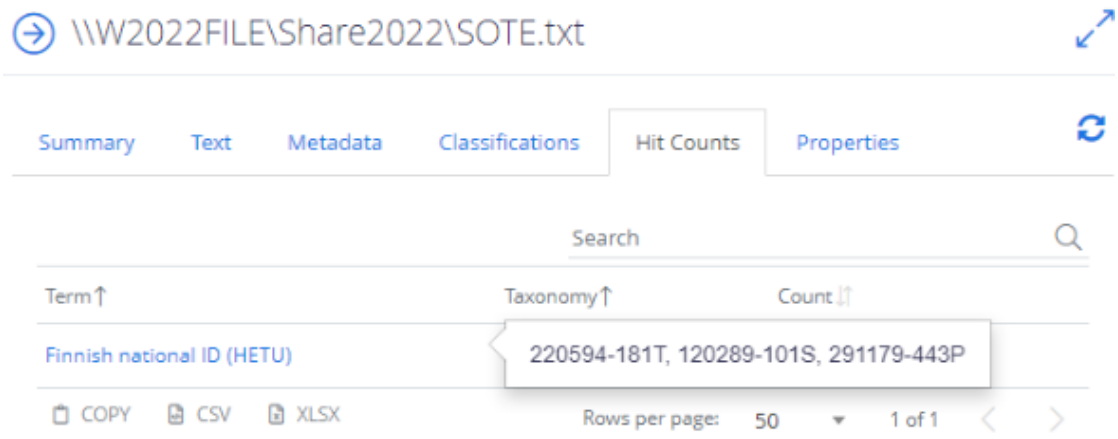
6.3.2 Netwrix Data Classificationin toiminta

Toisesta lähteestä lisätään testitiedosto (kuva 32), jonka sisään kirjoitetaan työkalulle tunnistettavia sanoja. Tiedoston lisäämisen jälkeen kansio skannataan ja klassifioidaan manuaalisesti uudestaan, jonka jälkeen tutkitaan tuloksia.



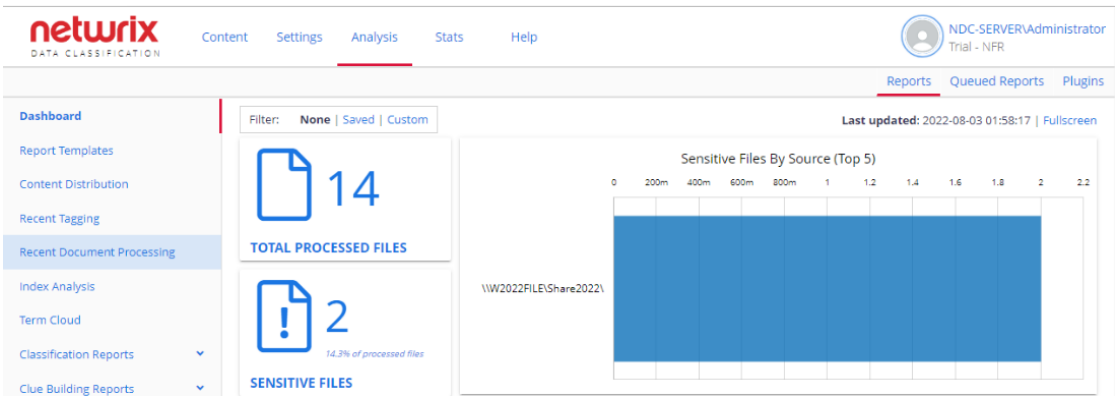
Kuva 32. Netwrix Data Classification testitiedosto

Kuvassa 33 näkyy, että tiedoston skannaus tuotti toivotut tulokset ja kaikki kolme henkilötunnusta huomioitiin sisällöstä.



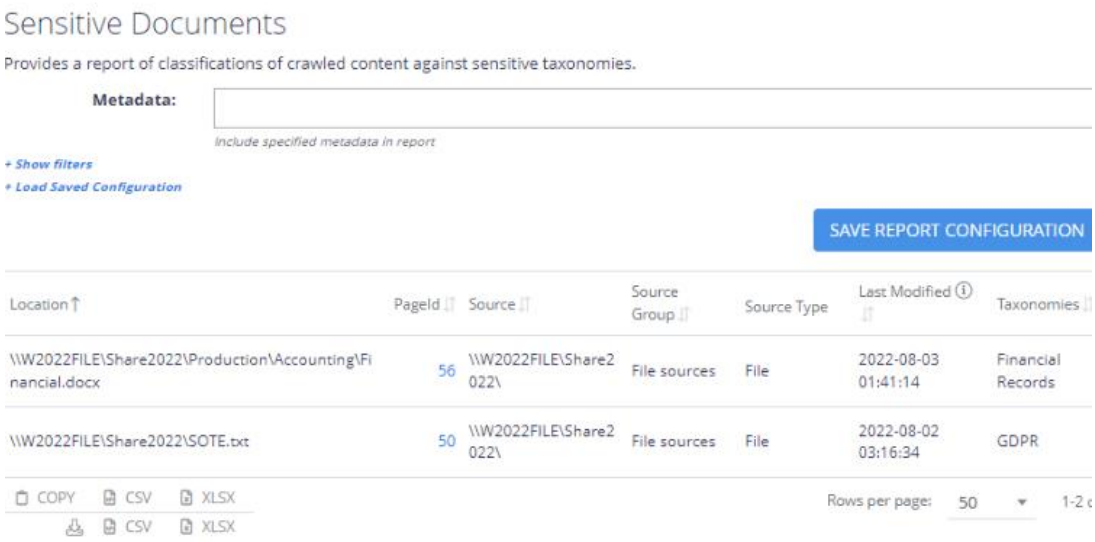
Kuva 33. Netwrix Data Classification testitiedoston klassifiointi

Testien vahvistamiseksi lisätään vielä tilitietoja tutkiva taksonomia ja luodaan IBAN-tilinumeroita sisältävä testitiedosto. Tämän jälkeen tuloksia tarkastellaan koko skannatusta ympäristöstä. Analysointi-välilehdeltä (kuva 34) näkee arkaluontoiseksi merkatut tiedostot, joita tällä hetkellä löytyy kaksi kappaletta.



Kuva 34 Analysointi-välilehti

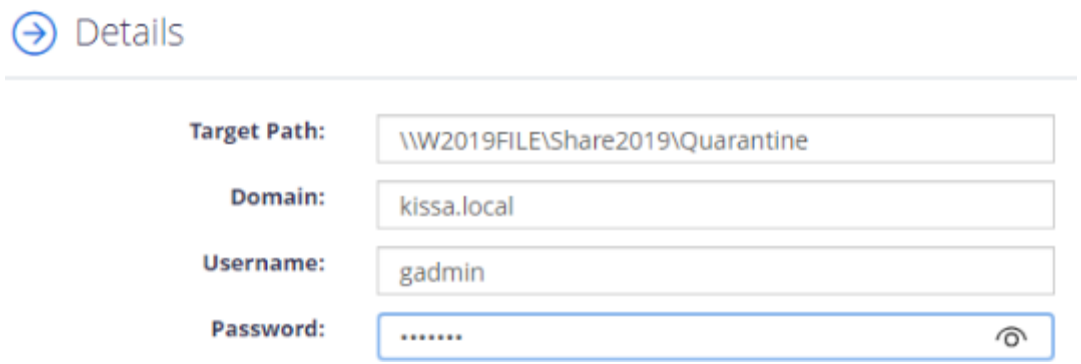
Arkaluontoisia tiedostoja ovat aiemmin luodut testitiedostot. Tiedoista näkee muun muassa tiedoston polun, tiedoston viimeisimmän muokkauspäivän ja taksonomiat, jotka aiheuttivat tiedoston klassifioinnin arkaluontoiseksi (kuva 35).



Kuva 35. Arkaluontoiset tiedostot

Seuraavaksi työkalusta testataan automatisoituja työnkulkuja. Tavoitteena on tehdä yksinkertainen automatisoitu työnkulku, joka siirtää arkaluontoista tietoa sisältävät tiedostot karanteenikansioon.

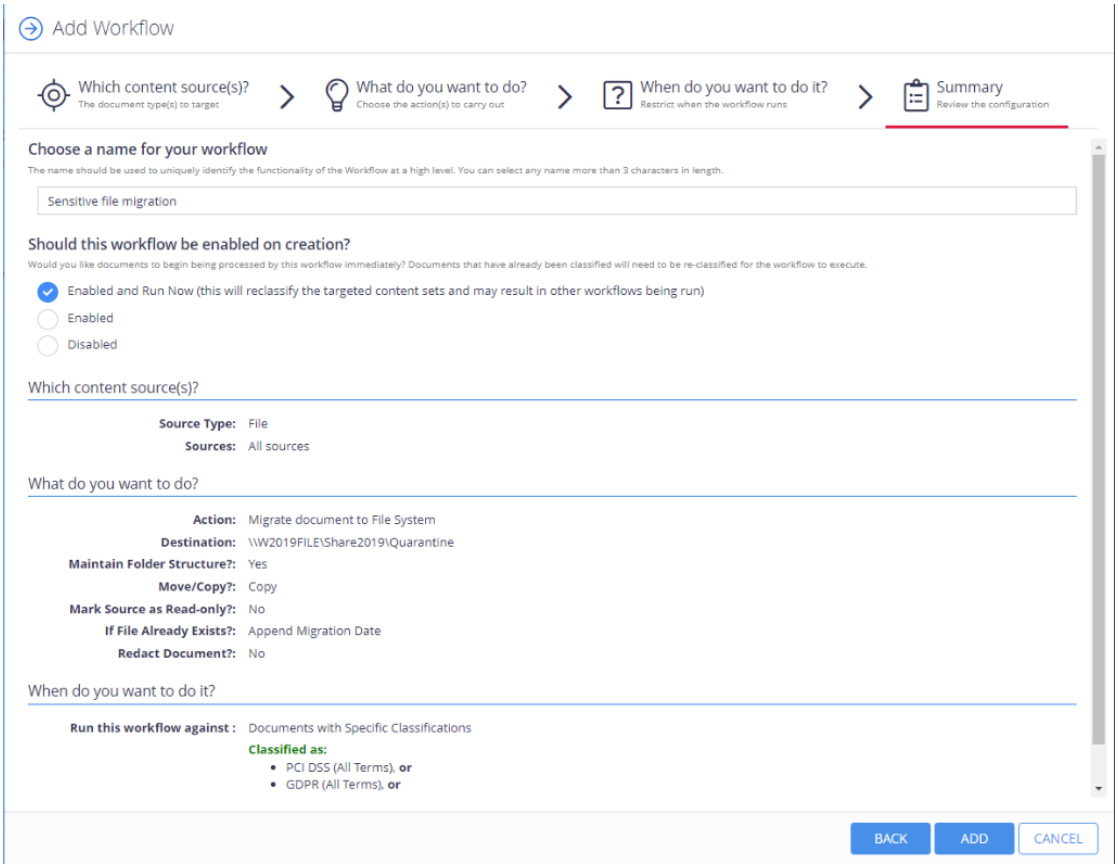
Ensin testiympäristössä testataan, toimiiko työnkulun tiedonsiirto tiedostopalvelimien välillä. Koska arkaluontoiset tiedostot ovat tällä hetkellä Windows Server 2022 -tiedostopalvelimessa, tiedonsiirtoa voidaan testata tekemällä karanteeni Windows Server 2019 -tiedostopalvelimeen. Työnkululle täytyy ensin konfiguroida karanteenina toimiva kansio. Karanteenille määritetään polku, toimialue ja käyttäjätunnukset, joita työnkulku käyttää (kuva 36).



Kuva 36. Konfiguraatio karanteenille

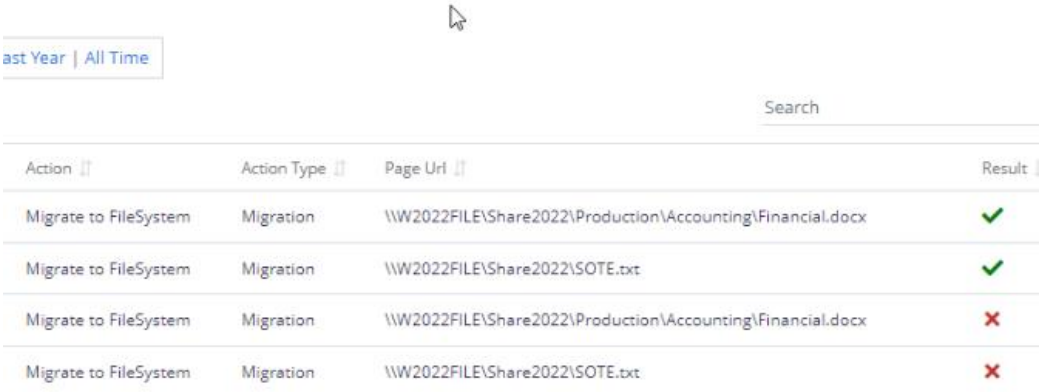
Seuraavaksi itse työnkulku (kuva 37) luodaan seuraavilla asetuksilla:

- Työnkulun aktiviteetti on dokumentin migraatio
- Mikäli kohteena on kansio, työnkulku kopioi myös alakansiot
- Kopioinnin jälkeen työnkulku ei poista tiedostoa vanhasta sijainnistaan
- Tiedoston nimen perään lisätään päivämäärä duplikaattien syntyessä
- Ei sähköposti-ilmoituksia tapahtuneista työnkuluista
- Työnkulku kopioi kaikki tiedostot, jotka on klassifioitu taksonomioiden GDPR, PCI DSS tai Financial Records mukaan



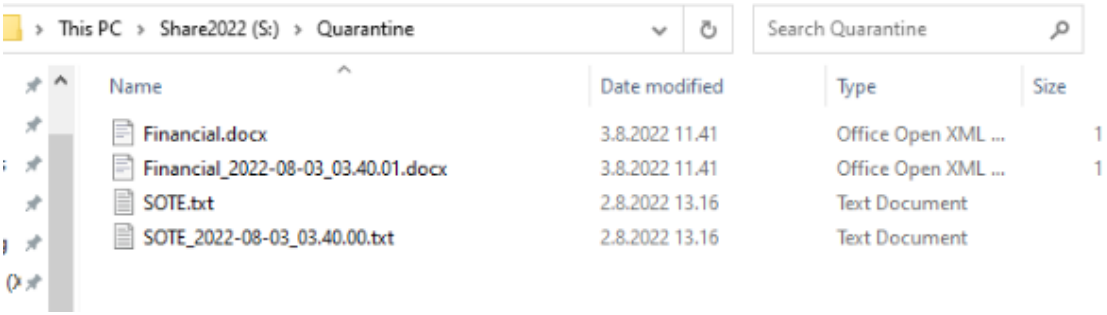
Kuva 37. Työnkulun yhteenveto ennen sen lisäämistä

Työnkulut lähtivät heti käyntiin, mutta molemmat epäonnistuivat. Epäonnistuneen työnkulun virheilmoitusta lukiessa ilmenee, että pääsy karanteenikansioon epäonnistui. Tämä johtuu mahdollisesti siitä, että karanteeni oli eri palvelimella, joten työnkulusta luodaan kopio ja asetetaan karanteeni samalle palvelimelle arkaluontoisten tiedostojen kanssa. Uusilla asetuksilla työnkulku onnistuu. (Kuva 38.)



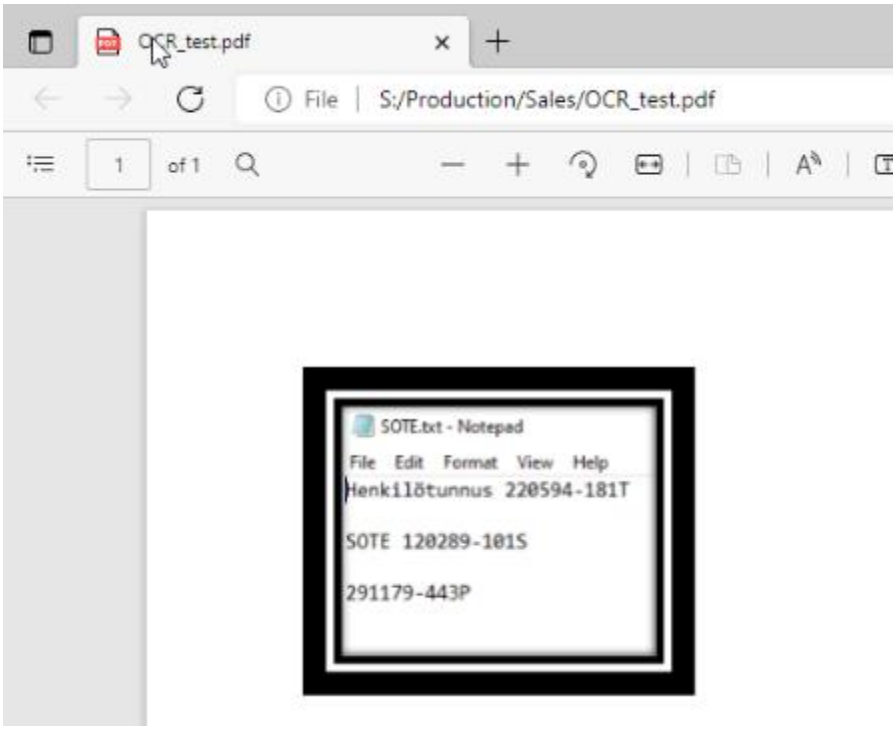
Kuva 38. Lokit onnistuneista ja epäonnistuneista työnkuluista

Uudelleen klassifioidut lähteet laukaisivat työnkulut toisen kerran. Tiedostojen duplikaattien perään ilmestyi päivämäärä, niin kuin aiemmin määriteltyjen asetuksien mukaan kuuluikin tapahtua (kuva 39).



Kuva 39. Tiedostojen duplikaatit karanteenissa

Lopuksi työkalulla testataan tekstintunnistusta kuvista. Lähteeseen luodaan PDF-tiedosto (kuva 40), johon ei kirjoiteta tekstiä ollenkaan, vaan sen sijaan liitetään kuvankaappaus aiemmasta testitiedostosta ja sen sisällöstä.



Kuva 40. Tekstintunnistukselle tehty testitiedosto

Kun tiedosto on skannattu, sen lisätiedoista näkee, miten työkalu tulkitsi tekstin. Testitiedoston skannaus ei ollut täydellinen, sillä työkalu tulkitsi joitain sanoja väärin, kuten kuvasta 41 näkee.

Kuva 41. Tunnistettu teksti

Työkalu ei myöskään osaa klassifioida testitiedostoa GDPR-taksonomian mukaan, vaikka se tunnistikin taksonomiaan viittaavia termejä oikein.

6.4 Kansion käyttöoikeuksien parhaat käytännöt

Koska toimeksiantajan eri tiedostojärjestelmille on monia järjestelmänvalvojia, niissä on paljon eroja keskenään. Tässä luvussa käydään läpi tutkittuja käytäntöjä.

6.4.1 Käyttöoikeuksien tasapainottelu

Koska kansio käyttää aina alinta oikeutta, kaikille käyttäjille voidaan antaa Full Control -käyttöoikeus jaetun resurssin käyttöoikeuksissa. Sen jälkeen käyttöoikeuksien rajoittaminen voidaan toteuttaa NTFS-puolella, missä rajoituksia voi tehdä paljon tarkemmin hyödyntämällä kansiokohtaisia rajoituksia sekä oikeuksien perintää. (Carsten 2018; Morgan 2021; Sys-Manage 2021; Netwrix s.a.)

Oikeuksia voidaan säätää sekä käyttäjä- että ryhmäkohtaisesti, mutta käytännöllisyyden kannalta kaikki rajoitukset kuuluisivat tehdä ryhmäkohtaisesti. Yksittäisiä käyttäjiä on helpompi siirrellä ryhmästä toiseen sen sijaan, että muokkaisi käyttäjien oikeuksia joka kerta (Murphy 2022). Suuressa yrityksessä yksittäisten käyttäjien käyttöoikeuksia on myös vaikea jäljittää ja niitä on hankalaa siivota pois, jos käyttäjä poistetaan Active Directorystä (Nikolaisen 2018).

6.4.2 Access-Based Enumeration

Access-Based Enumeration (ABE) estää käyttäjiä näkemästä kansioita ja tiedostoja, joihin heillä ei ole käyttöoikeuksia. Tämä teknologia auttaa piilottamaan arkaluontoista tietoa. (NetApp 2022.)

Nikolaisen (2018) suosii ABE:n käyttöön ottamista, koska se helpottaa käyttäjien työskentelyä. Mikäli tiedostopalvelimella on monia kymmeniä kansioita, joista vain muutama on tarkoitettu yhdelle käyttäjälle, halutut kansiot löytävät helpommin.

Smith (2020) huomioi, että jo pelkästään kansion nimi voi sisältää arkaluontoista informaatiota, jonka takia ne kannattaisi piilottaa tarpeettomilta silmiltä. Tietoturvaseikkojen lisäksi hän kuitenkin kehottaa ensin testaamaan, kuinka rankasti ABE rasittaa palvelimen suorituskykyä.

6.4.3 Dokumentointi

Dokumentoimalla kaikki prosessit, jotka sisältävät tiedostojärjestelmien luomista tai niiden muuttamista, saadaan viitekohta tuleville prosesseille. Dokumentaatiota hyödyntämällä uudet ja muutetut ympäristöt voidaan pitää rakenteeltaan samanlaisina. Tämä kaikki auttaa myös järjestelmänvalvojia yhteistyössä. (Nikolaisen 2018.)

Hyvä dokumentaatio säästää työntekijän aikaa. Työntekijä löytää etsimäänsä tietoa nopeammin hyvin järjestellystä kansiosta kuin esimerkiksi vanhoista sähköposteista. Mikäli yritykseen tulee uusi työntekijä, perehdytyksen tukena voidaan käyttää dokumentaatiota. Kun uusi työntekijä saa vastauksia kysymyksiinsä dokumentaatiosta sen sijaan, että kysyisi perehdyttäjältä, hän säästää taas aikaa. (Atlassian s.a.)

7 TULOKSET

Tiedostopalvelimien ylläpitoa helpotetaan automaatiolla. Järjestelmänvalvojan on mahdotonta valvoa manuaalisesti tiedostojakojen sisältöä, kun niiden sisältöä tuottavat kymmenet tai jopa sadat käyttäjät. Myös käyttäjäryhmien ylläpitämistä saatetaan laiminlyödä, jos ajastetut raportit eivät ole muistuttamassa kerääntyneistä turhista käyttöoikeuksista. Testatuissa työkaluissa melkein kaikki toiminnot pystyttiin automatisoimaan.

Hyvä dokumentaatio kertoo logiikan ja käyttötarkoituksen jokaiselle käyttäjäryhmälle. Mikäli sekavia käyttäjäryhmiä tarvitsee järjestellä dokumentaatiolla ja IAM-työkalun ominaisuuksilla, kuten päällekkäisten käyttöoikeuksien tarkistuksella, voidaan vertailla käyttäjäryhmien alkuperäistä käyttötarkoitusta ja nykyistä käyttötapaa.

Vähimpien oikeuksien periaatteella voidaan pitää palvelinympäristö turvallisena ilman, että työntekijöiden työskentelystä tehdään liian hankalaa. Periaatteen tarkoitus ei ole estää työntekijää käyttämästä hänelle tarpeellisia työkaluja tai käyttöoikeuksia, vaan karsia kaikki ylimääräinen pois. Vähimpien oikeuksien periaatetta voidaan toteuttaa IAM-työkalujen automaattisilla

raporteilla käyttöoikeuksista. Access-Based Enumeration puolestaan tukee sekä käytännöllisyyttä että turvallisuutta.

Käyttäjäryhmien ja tiedostojärjestelmien hallintaan tarkoitetut työkalut säästävät järjestelmänvalvojien aikaa, täyttävät tietoturvavaatimuksia ja tuovat uusia näkökulmia käyttäjäryhmien ongelmien ratkomiseen. Työkalujen avulla järjestelmiä voidaan myös hallita yhdestä keskitetystä pisteestä.

8 JOHTOPÄÄTÖKSET

Käyttöoikeuksien tutkitut parhaat käytännöt eivät itsessään tuo mitään uutta tietoa, vaan enemmänkin vahvistavat toimeksiantajan nykyisiä näkemyksiä. NTFS-käyttöoikeuksia käytetään jo ensisijaisesti ja käyttöoikeuksia jaetaan käyttäjäryhmätasolla käyttäjätason sijaan. Myös Access-Based Enumeration on otettu käyttöön osassa tiedostojaoista. Dokumentointi on luonnollinen osa prosesseja sekä yleisesti että toimeksiantajan kohdalla. Sen laiminlyönti voi laskea prosessien laatua, joten sen hyötyjä tuotiin esiin käytäntöjen tutkinnassa.

Testitulosten luotettavuutta heikentää tietenkin testiympäristön koko. Vaikka työkalut tekivät tehtävänsä onnistuneesti, täytyy harkita, miten ne toimisivat tuotantoympäristössä. Skannattavien käyttäjäryhmien ja analysoitavien tiedostojen määrä kasvaa satoja kertoja suuremmaksi, kun siirrytään toimeksiantajan ympäristöön. Toisaalta työkalujen vaikutus ja tärkeys on varmasti paljon selvempää, kun ne otetaan käyttöön suuressa ja korjausta vaativassa ympäristössä.

IAM- ja DLP-työkalut tarvitsevat myös omat käyttäjätilinsä ja käyttöoikeutensa, jotta ne kykenevät tekemään toimintoja tiedostojaoissa tai Active Directoryssä. Testiympäristössä työkalujen käyttäjätileille annettiin täydet oikeudet, jotta testit saataisiin tehtyä helposti ja nopeasti. Tuotantoympäristössä työkalujen käyttöoikeuksia täytyisi rajata huolellisesti. Mikäli IAM- tai DLP-työkalujen käyttämät tilit kaapattaisiin, nämä työkalut aiheuttaisivat juuri sitä vahinkoa, mitä niillä alun perin yritettiin estää.

Windows File Auditin käyttöönotto testiympäristössä onnistui alle tunnissa, eikä se aiheuta pienen levytilan menetyksen lisäksi minkäänlaista haittaa tiedostopalvelimelle. Kaikista tämän työn ehdotuksista Windows File Auditin täytyisi olla ensimmäinen asia mihin perehtyä. Vaikka lokitietoja voi olla hankalaa tutkia Event Vieweristä, on silti järkevää ottaa käyttöön edes joku väliaikainen tapa monitoroida toimintaa tiedostojaoissa.

8.1 IAM-työkalu

Testien jälkeen SolarWinds ARM:n voidaan todeta kykenevän ainakin seuraaviin toimintoihin:

- Käyttäjäryhmien käyttöoikeuksien tutkiminen kansiokohtaisesti
- Käyttöoikeuksien muutoksien tutkiminen
- Yksittäisen käyttäjän pääsyn tutkiminen
- Epäaktiivisten käyttäjien löytäminen
- Päällekkäisten käyttöoikeuksien löytäminen
- Kaiken aiemmin mainitun automatisoitu raportointi
- Käyttöoikeuksien visualisointi interaktiivisella kaaviolla

Tuloksien jälkeen täytyy miettiä, kuinka tarpeellisia IAM-työkalun toiminnot ovat. Samankaltaisia toimintoja voidaan myös toteuttaa esimerkiksi Windowsin komentorivityökalulla PowerShell, joka on asennettu oletuksena Windows Server -palvelimiin. Kuten SolarWinds ARM, myös PowerShell voi etsiä epäaktiivisia käyttäjiä tai käyttäjäryhmien oikeuksia ja jäseniä. PowerShelliin tai muihin komentorivityökaluihin verrattuna IAM-työkalujen vahvuudet ovat toimintojen yksinkertaistaminen ja datan visualisointi, jotka johtavat ylläpidon helpottamiseen.

IAM-työkalun hyödyllisyys yleisesti ottaen on todistettu, mutta SolarWindsin luotettavuutta täytyy kyseenalaistaa. Vuonna 2020 SolarWinds joutui kyberhyökkäyksen kohteeksi ja SolarWindsin asiakkaiden dataa päätyi hakkereiden käsiin (Oladimeji & Kerner 2022). Tästä syystä muita mahdollisia vaihtoehtoja täytyy vielä harkita SolarWinds ARM:n sijaan, mikäli toimeksiantajan ympäristöön otetaan käyttöön IAM-työkalu.

8.2 DLP-työkalu

Netwrix Data Classification skannaa nopeasti tekstiä ja kuvia tiedostojaoista. Se tunnistaa tehokkaasti arkaluontoisen tiedon ja merkitsee ne oikeilla taksonomioilla myöhemmin tarkasteltavaksi. Prosessit voidaan automatisoida ja tarvittaessa niistä syntyvät hälytykset voidaan lähettää eteenpäin sähköpostiin.

Koska työkalun kokeiluversiolla oli rajattu aika, siitä ei keretty varmistaa tiedon siirron toimivuutta palvelimien välillä. Kaiken kaikkiaan työkalusta löytyi kaikki ominaisuudet, mitä oli odotettavissakin. Täytyy myös huomioida, että toisin kuin IAM-työkalun toimintoja, DLP-työkalun toimintoja olisi erittäin haastavaa toteuttaa esimerkiksi PowerShellillä. Mikäli toimeksiantajan ympäristöön aletaan implementoimaan DLP-työkalua, Netwrix Data Classificationia voidaan pitää hyvänä ehdokkaana.

9 POHDINTA

Työlle asetetut tavoitteet saavutettiin enimmäkseen. Tutkitut työkalut toimivat odotusten mukaisesti, vaikka DLP-työkalun testit jäivätkin hieman puutteellisiksi kokeiluversion aikarajan takia. Jotain muuta IAM-työkalua olisi ehkä harkittu testeille, mikäli SolarWindsin omista tietoturvaongelmista olisi tiedetty ajoissa. Myös toimeksiantajan olemassa olevia käytäntöjä saatiin vahvistettua, kun kaikki tutkitut parhaat käytännöt toimivat ensisijaisesti samoilla menetelmillä.

Työn aihe oli alun perin tarkoitus toteuttaa täysin teoreettisella pohjalla. Tässä muodossa sitä oli kuitenkin hyvin vaikea rajata. Työn tarkoitusta alkoi hahmottamaan paljon paremmin, kun toimeksiantajaa uudelleen haastatellessa otettiin puheeksi työssä mainittuja periaatteita ajavat työkalut. Työn muodon muutoksestakin seurasi omat haasteensa. Vaikka hyviä työkaluja löytyi paljon, harvalla niistä oli ilmaisia kokeiluversioita. Niistä työkaluista, joita vihdoin pääsi kokeilemaan, ei löytynyt niiden omien käsikirjojen lisäksi paljoa dokumentaatiota. Tästä syystä alustava tutustuminen työkaluihin kesti hieman toivottua kauemmin.

Xamkin virtuaalisesta testiympäristöstä oli paljon apua työn toteutuksen kanssa. Ymmärrettävistä syistä siellä tarjolla olevat resurssit olivat rajattuja ja

niiden hallintaan sai käyttää välillä aikaa. Xamkin henkilökunta kuitenkin auttoi aina tarvittaessa kaikkien virtuaalilaboratorion teknisten ongelmien kanssa ja lopulta testiympäristö olikin yksi työn tärkeimpiä osia.

Ennen työn aloittamista tietämys aiheesta oli puutteellista, mikä sai kyseenalaistamaan työn tärkeyttä. Epäröinti loppui kuitenkin, kun oli tutkinut ja oppinut, minkälaista vahinkoa kaapattu käyttäjätili tai vuotanut arkaluontoinen data voi aiheuttaa yritykselle. Tämä työn aikana sisäistetty tieto ei omalla kohdalla mene hukkaan, koska tutkitut vaarat eivät ole olemassa pelkästään tiedostopalvelimissa ja käyttäjätileissä, vaan myös muualla tietotekniikan osa-alueilla.

Mikäli tutkimusta jatkettaisiin eteenpäin, muita IAM- tai DLP-työkaluja voitaisiin vertailla keskenään. Työn aikana tutkitut vaihtoehdot vaikuttivat alustavasti samankaltaisilta, mutta työkalujen ominaisuudet toimivat varmasti eri tavoin, kun konfiguraatioissa mennään syvemmälle tasolle. Toinen hyvä jatkotutkimuksen kohde on Windows File Audit. File Audit pystyy keräämään todella yksityiskohtaista tietoa kansion tapahtumista, mutta sen suurimpana ongelmana on lokitietojen tutkimisen haastavuus. Vaikka näiden tietojen tutkimiselle on olemassa kolmannen osapuolen työkaluja, olisi paljon suotavampaa käyttää Windowsin sisäänrakennettuja työkaluja. Esimerkiksi PowerShell voi etsiä Windowsin lokitietoja ja niiden ulostuloa voidaan säätää omien tarpeiden mukaisesti. Tämä voisi tuoda lisää mahdollisia ratkaisuja tiedostojärjestelmien ylläpidon helpottamiseen.

LÄHTEET

Atlassian. s.a. The importance of documentation. WWW-dokumentti. Saatavissa: https://www.atlassian.com/work-management/knowledge-sharing/documentation/importance-of-documentation [viitattu 14.10.2022].

Carsten. 2018. 7 BEST PRACTICES IN MANAGING NTFS PERMISSIONS. WWW-dokumentti. Saatavissa: https://blog.foldersecurityviewer.com/7-best-practices-in-managing-ntfs-permission/ [viitattu 14.10.2022].

CyberArk. s.a. Principle of Least Privilege. WWW-dokumentti. Saatavissa: https://www.cyberark.com/what-is/least-privilege/ [viitattu 14.10.2022].

Gittlen, S. & Rosencrance, L. s.a. What is identity and access management? WWW-dokumentti. Saatavissa: https://www.techtarget.com/searchsecurity/definition/identity-access-management-IAM-system [viitattu 14.10.2022].

IBM. s.a. Why is IAM important? WWW-dokumentti. Saatavissa: https://www.ibm.com/topics/identity-access-management [viitattu 14.10.2022].

Imperva. s.a. Data Breach. WWW-dokumentti. Saatavissa: https://www.imperva.com/learn/data-security/data-breach/ [viitattu 14.10.2022].

Ingalls, S. 2021. What is a File Server & How Does It Work? WWW-dokumentti. Saatavissa: https://www.serverwatch.com/guides/what-is-a-file-server-how-does-it-work/ [viitattu 14.10.2022].

Kananen, J. 2017. Kehittämistutkimus interventiotutkimuksen muotona. Jyväskylä: Jyväskylän ammattikorkeakoulu.

Kaspersky. s.a. How Data Breaches Happen. WWW-dokumentti. Saatavissa: https://www.kaspersky.com/resource-center/definitions/data-breach [viitattu 14.10.2022].

Microsoft. 2021a. NTFS overview. WWW-dokumentti. Saatavissa: https://docs.microsoft.com/en-us/windows-server/storage/file-server/ntfs-overview [viitattu 14.10.2022].

Microsoft. 2021b. Security auditing. WWW-dokumentti. Saatavissa: https://docs.microsoft.com/en-us/windows/security/threat-protection/auditing/security-auditing-overview [viitattu 14.10.2022].

Microsoft. 2021c. Basic security audit policies. WWW-dokumentti. Saatavissa: https://docs.microsoft.com/en-us/windows/security/threat-protection/auditing/basic-security-audit-policies [viitattu 14.10.2022].

Microsoft. 2022. Learn about data loss prevention. WWW-dokumentti. Saatavissa: https://docs.microsoft.com/en-us/microsoft-365/compliance/dlp-learn-about-dlp?view=o365-worldwide [viitattu 14.10.2022].

Morgan M. 2021. Your Guide to NTFS Vs. Share Permissions Best Practices. WWW-dokumentti. Saatavissa: https://www.globalknowledge.com/us-en/resources/resource-library/articles/your-guide-to-ntfs-vs-share-permissions-best-practices/ [viitattu 14.10.2022].

Murphy, P. 2022. What's the Difference Between Share and NTFS Permissions? WWW-dokumentti. Saatavissa: https://www.lepide.com/blog/whats-the-difference-between-share-and-ntfs-permissions/ [viitattu 14.10.2022].

NetApp. 2022. Provide folder security on shares with access-based enumeration overview. WWW-dokumentti. Saatavissa: https://docs.netapp.com/us-en/ontap/smb-admin/provide-security-access-based-enumeration-task.html [viitattu 14.10.2022].

Netwrix. s.a. Netwrix Data Classification. WWW-dokumentti. Saatavissa: https://www.netwrix.com/data_classification_software.html [viitattu 14.10.2022].

Netwrix. s.a. NTFS Permissions Management Best Practices. WWW-dokumentti. Saatavissa: https://www.netwrix.com/ntfs_permissions_management.html [viitattu 14.10.2022].

Nikolaisen, N. 2018. NTFS Permissions Best Practices: How to Set Permissions Correctly! WWW-dokumentti. Saatavissa: https://www.tenfold-security.com/en/set-ntfs-permissions/#tenfold-toc-anchor-12 [viitattu 14.10.2022].

Oladimeji, S. & Kerner S. M. SolarWinds hack explained: Everything you need to know. WWW-dokumentti. Saatavissa: https://www.techtarget.com/whatis/feature/SolarWinds-hack-explained-Everything-you-need-to-know [viitattu 14.10.2022].

Smith, R. 2020. Improve File Server Security Using Access-Based Enumeration (ABE). WWW-dokumentti. Saatavissa: https://www.lepide.com/blog/improve-file-server-security-using-abe/ [viitattu 14.10.2022].

Sys-Manage. 2021. How Share, NTFS Permissions and Inheritance Actually Work. WWW-dokumentti. Saatavissa: https://www.sys-manage.com/Blog/how-share-ntfs-permissions-and-inheritance-actually-work#windows-access-check [viitattu 14.10.2022].

Trellix. s.a. What Is DLP and How Does It Work? WWW-dokumentti. Saatavissa: https://www.trellix.com/en-us/security-awareness/data-protection/how-data-loss-prevention-dlp-technology-works.html [viitattu 14.10.2022].