jamk

Tietoturvakontrollit – Labra 4

Ryhmä 3

Juha-Matti Hietala

Markus Pollari

Topi Liljeqvist

Maija Virta

Oppimistehtävä

Helmikuu 2023

Tekniikan ala

Tieto- ja viestintätekniikan tutkinto-ohjelma (AMK)

jamk | Jyväskylän ammattikorkeakoulu
University of Applied Sciences

Sisältö

Kuvat

1 Johdanto

Labra nelosen tarkoituksena on harjoitella erilaisten käyttäjien ja ryhmien tunnistamista sekä sääntöjä, jota niille voidaan antaa, ja tätä kautta tutustua user-ID:n sekä captive portalin käyttöön.

Harjoituksessa pyritään luomaan ympäristömme www palvelimelle tunnistautuminen niin, että vain tietyt käyttäjät pääsevät sisäverkosta www-sivuilemme. Käytämme tunnistautumiseen harjoituksessa hyväksi paloaltossa toimivaa captive portalia. Asetamme DMZ-zonelle säännön, joka määrää kirjautumisen captive portalin kautta aina kun koitetaan kirjautua tuntemattomalla käyttäjällä www-sivuillemme.

Tunnistautuminen tehdään harjoituksessa toimimaan paloaltossa luoduilla local tunnuksilla, sekä ympäristömme AD:ssa sijaitsevilla käyttäjillä. Jotta AD käyttäjätunnukset saadaan toimimaan tunnistautumiseen, pitää AD integroida paloalton kanssa toimivaksi. Harjoitustyössä dokumentoidaan kaikki tehdyt toimenpiteet sekä lisäksi käydään läpi teoria User-Id:stä, PaloAlto captive portalista ja LDAP:ista.

2 TEORIA

2.1 User-ID

USER-ID on Palo Alto Networksin tietoturva-alustan ominaisuus, jonka avulla organisaatiot voivat tunnistaa käyttäjät ja valvoa suojauskäytäntöjä heidän henkilöllisyytensä perusteella. Tämä ominaisuus tarjoaa näkyvyyden siitä, kuka käyttää verkkoa, mitä he tekevät ja mitä resursseja he käyttävät. Se toimii kartoittamalla verkon toimintaa tietylle käyttäjälle tai ryhmälle pelkän IP-osoitteen sijaan. (User-ID N.d.)

USER-ID:tä voidaan käyttää integroitaessa Active Directoryn, LDAP:n tai muiden hakemistopalvelujen kanssa käyttäjien automaattiseen tunnistamiseen ja todentamiseen heidän kirjautumistietojensa perusteella. Se voidaan myös integroida muihin tietoturvateknologioihin, kuten VPN-

verkkoihin ja verkkovälityspalvelimiin, tarjotakseen keskitetyn näkymän käyttäjien toiminnasta useissa suojaustyökaluissa. (User-ID N.d.)

Hyödyntämällä USER-ID:tä organisaatiot voivat parantaa tietoturvaansa ottamalla käyttöön yksityiskohtaisempia kulunvalvontakäytäntöjä, tunnistamalla ja tutkimalla tietoturvahäiriöitä nopeammin ja vähentämällä sisäpiiriuhkien riskiä. (User-ID N.d.)

2.2 Palo Alto Captive Portal

Captive-portaali on verkkosivu, jolle tunnistamaton käyttäjä uudelleenohjataan, kun hän muodostaa yhteyden vieraaseen SSID:hen (service set identifier). Käyttäjä voi päästä internetiin, kun hän on onnistuneesti tunnistautunut/kirjautunut. (Captive Portal Modes 2023.)

Palo Alto palomuurin Captive Portal-tila määrittää, miten palomuuri kaappaa verkkotodennuspyynnöt:

Läpinäkyvä (Mode: Transparent): Palomuuri sieppaa selainliikenteen todennuskäytännön säännön mukaan ja esiintyy alkuperäisenä kohde URL-osoitteena ja lähettää HTTP 401:n todennuksen käynnistämiseksi. Koska palomuurilla ei kuitenkaan ole kohde-URL-osoitteen todellista varmennetta, selain näyttää varmennevirheen käyttäjille, jotka yrittävät päästä suojatulle sivustolle. (Captive Portal Modes 2023.)

Uudelleenohjaus (Mode: Redirect): Uudelleenohjaustila vaaditaan, jos käytetään monivaiheista todennusta Captive Portal -käyttäjien todentamiseen (Captive Portal Modes 2023).

Palomuuri sieppaa tuntemattomat (HTTP tai HTTPS) istunnot ja uudelleenohjaa ne palomuurin Layer 3 -liittymään käyttämällä HTTP 302 -uudelleenohjausta todennuksen suorittamiseksi. Tämä on ensisijainen tila, koska se tarjoaa paremman loppukäyttäjäkokemuksen. Se vaatii kuitenkin ylimääräisiä Layer 3 -määrityksiä.

Uudelleenohjaustilan etuna on se, että se mahdollistaa istuntoevästeiden käytön, mikä mahdollistaa käyttäjän jatkavan selaamista todennetuille sivustoille ilman tarvetta kartoittaa uudelleen aina, kun aikakatkaisut umpeutuvat. Tämä on erityisen hyödyllistä käyttäjille, jotka liikkuvat IP-osoitteesta toiseen (esimerkiksi yrityksen lähiverkosta langattomaan verkkoon), koska heidän ei

tarvitse todentaa uudelleen IP-osoitteen muuttuessa niin kauan kuin istunto pysyy auki. (Captive Portal Modes 2023.)

2.3 LDAP

LDAP on ohjelmistoprotokolla, jonka avulla voidaan paikantaa tietoja henkilöistä ja muista resurs-seista, kuten tiedostoista ja laitteista verkossa. Verkko voi olla julkinen internet tai sisäverkko. LDAP on kevyt versio DAP:sta (Directory Access Protocol), koska se käyttää muita protokollia vähemmän koodia. DAP on osa X.500 standardia hakemistopalveluihin verkossa. Yleisin käyttö LDAP:lle on keskitetty paikka todennukselle, eli se varastoi käyttäjänimiä ja salasanoja. Eri ohjelmat ja palvelut voivat liitännäisien avulla käyttää LDAP:ta käyttäjän todentamiseen. (Gillis 2022)

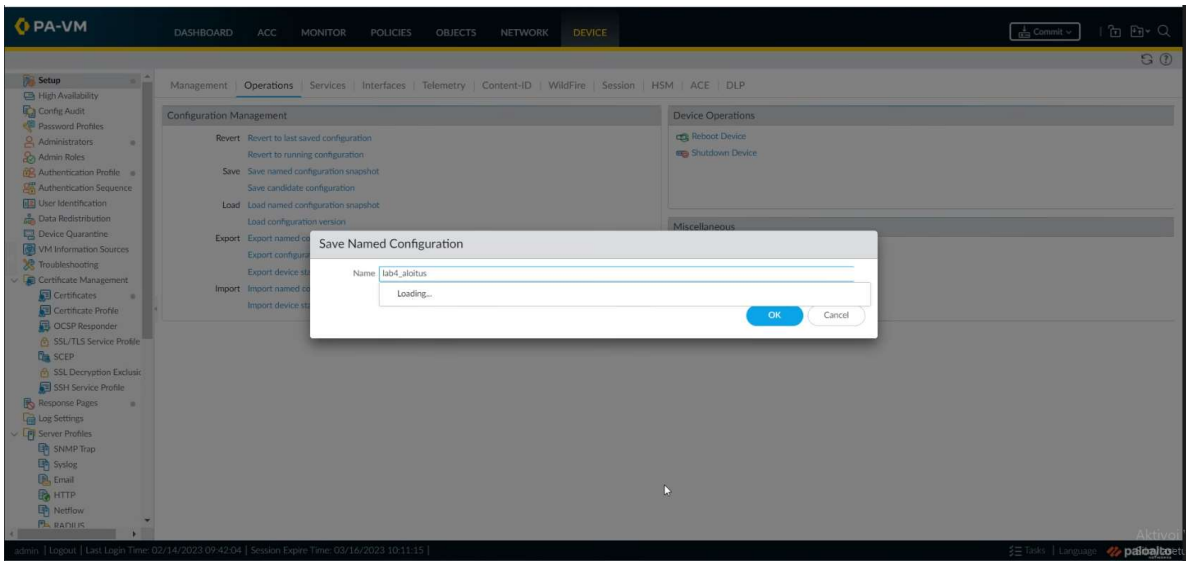
LDAP:ta käytetään Microsoftin Active Directoryssa. Active Directory sisältää tiedot kaikista käyttäjätileistä verkon sisällä. Jokaista käyttäjätiliä kohdellaan objektina ja jokaisella objektilla on useita ominaisuuksia, kuten esimerkiksi sähköpostiosoite, etunimi, sukunimi ja niin edelleen. Kaikki tämä suuri määrä kryptistä tietoa on olemassa toimialueen ohjainkoneessa (domain controller), eli Active Directoryssa. LDAP:n päätehtävä on poimia tämä tieto käytettävässä muodossa. (Gillis 2022)

Paloaltossa LDAP todennus voidaan määritellä loppukäyttäjille sekä palomuurin ja Panoraman järjestelmänvalvojille. Asettamalla palomuuri ottamaan yhteys LDAP serveriin, mahdollistaa se käytäntöjen määrittämisen käyttäjien ja käyttäjäryhmien perusteella pelkän IP-osoitteen sijaan. (LDAP 2023)

3 DOKUMENTOINTI

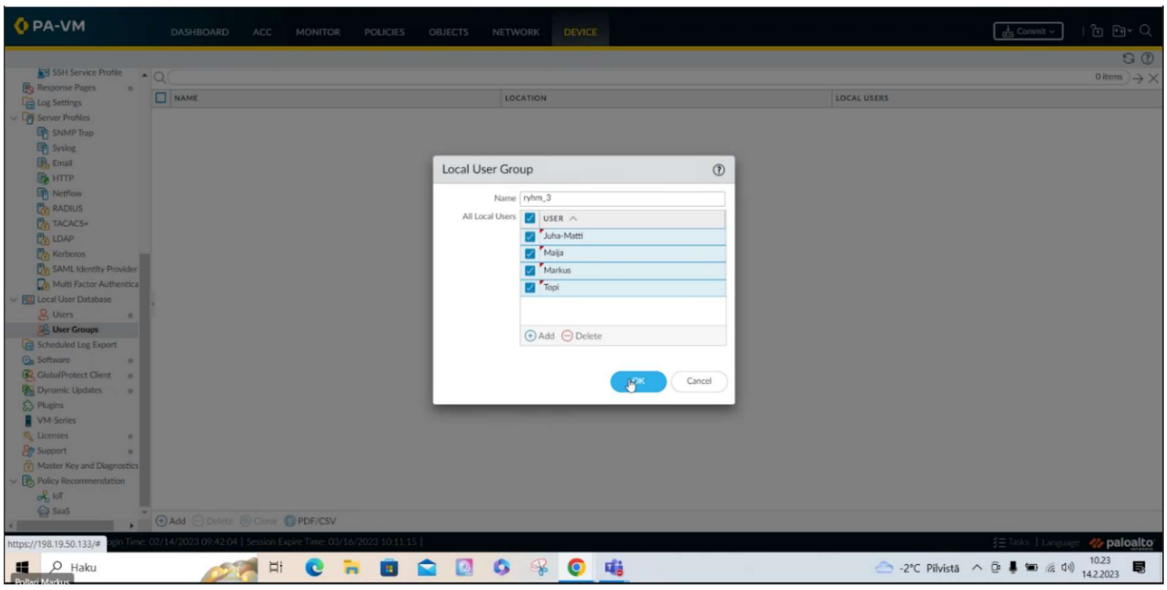
3.1 Local tunnukset

Labra 4 aloitettiin ottamalla snapshot alkutilanteesta, tässä labrassa snapshotin otto oli erityisen tärkeää, sillä labrassa tehtäviä muutoksia ei tulla pitämään ympäristössä.



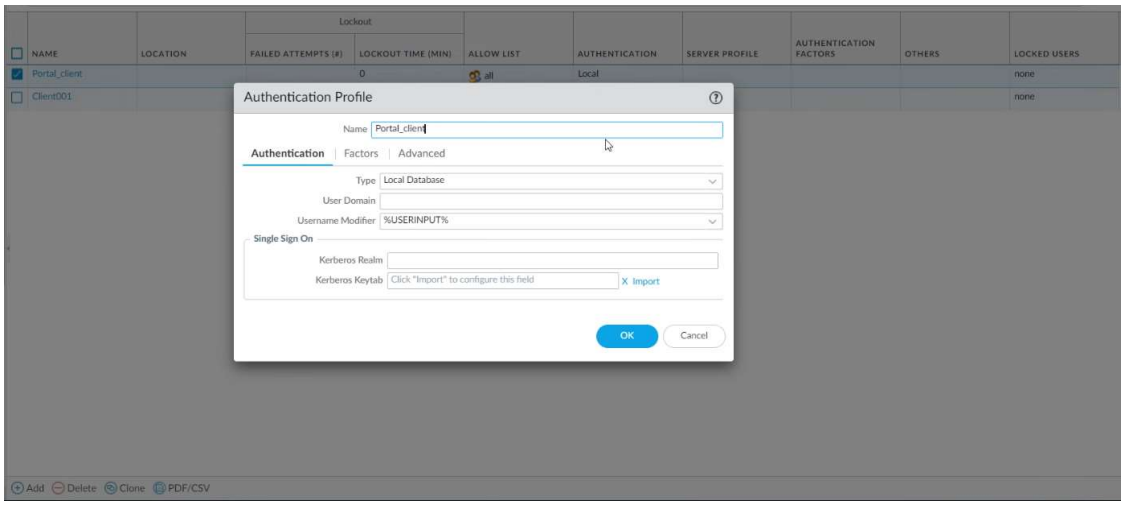
Kuva 1. Snapshot alkutilanteesta

Luotiin uusi Local User Group ja lisättiin sinne aiemmin luomamme Local tunnukset. Esitetty kuvassa 2.



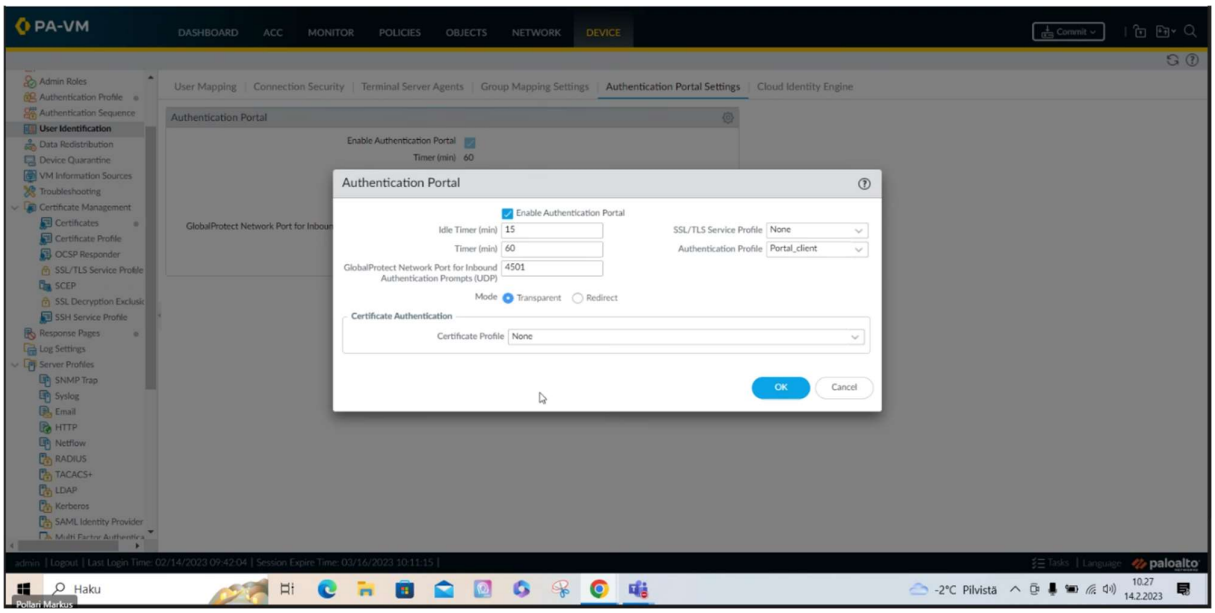
Kuva 2. Local User Group luonti.

Päätimmme käyttää jo aiemmin luotua VPN authentication profilea. Esitetty kuvassa 3.



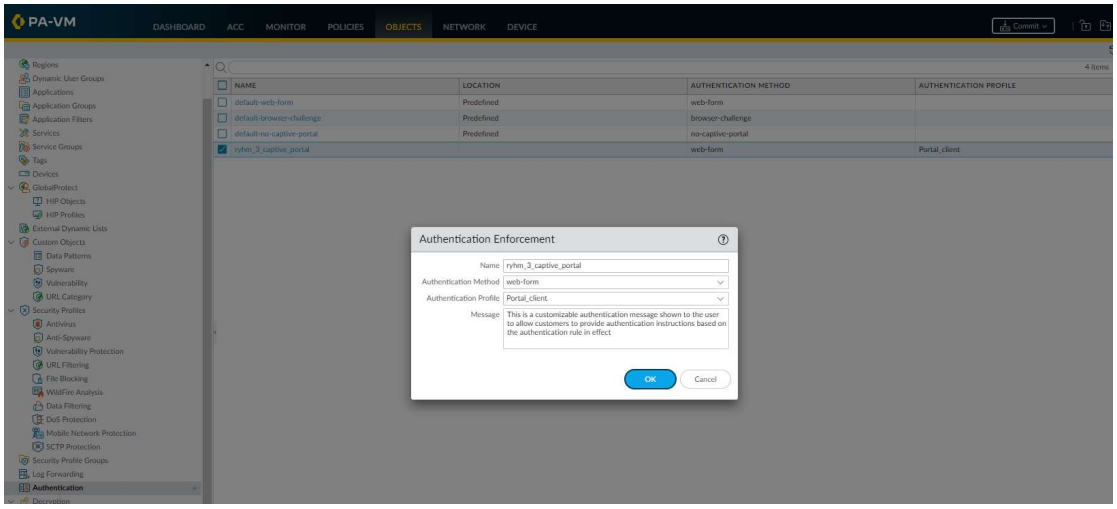
Kuva 3. Authentication profile

Otettiin käyttöön Authentication Portal ja asetettiin sille aiemmin luotumme VPN authentication profile Portal_client. Esitetty kuvassa 4.

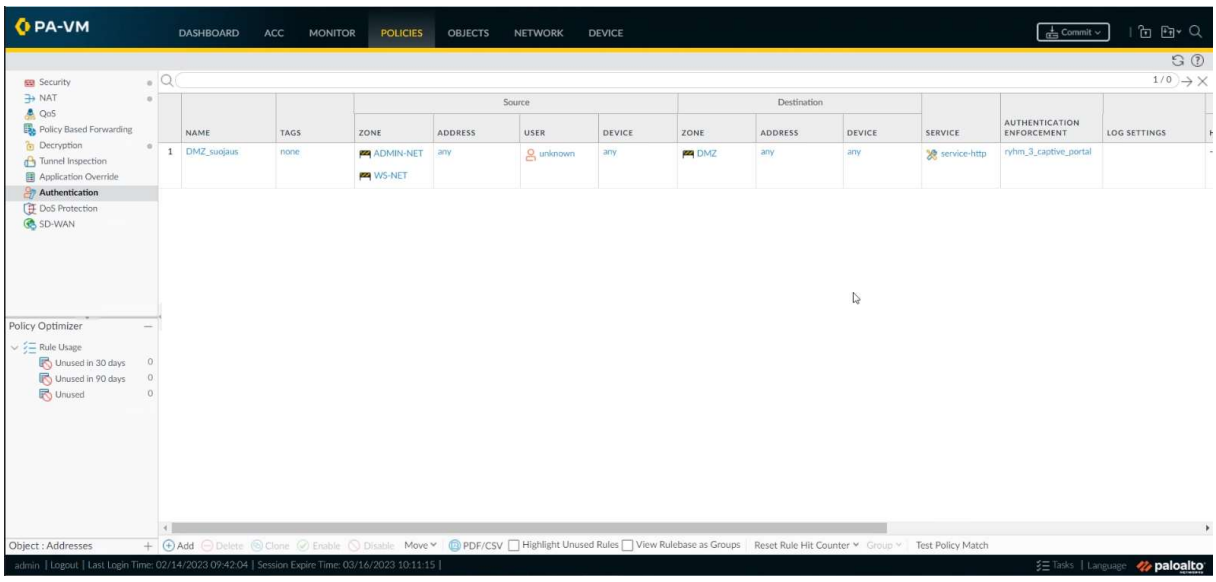


Kuva 4. Authentication Portal luonti

Luotiin uusi tunnistautumis tapa nimeltä ryhm_3_captive_portal sekä lisättiin se luomaamme sääntöön jolla vaadittiin tunnistautuminen. Tunnistautuminen vaaditaan kirjautuessa ympäristömme www palvelimelle Admin tai WS netistä tuntemattomalla käyttäjällä. Esitetty kuvissa 5 ja 6.

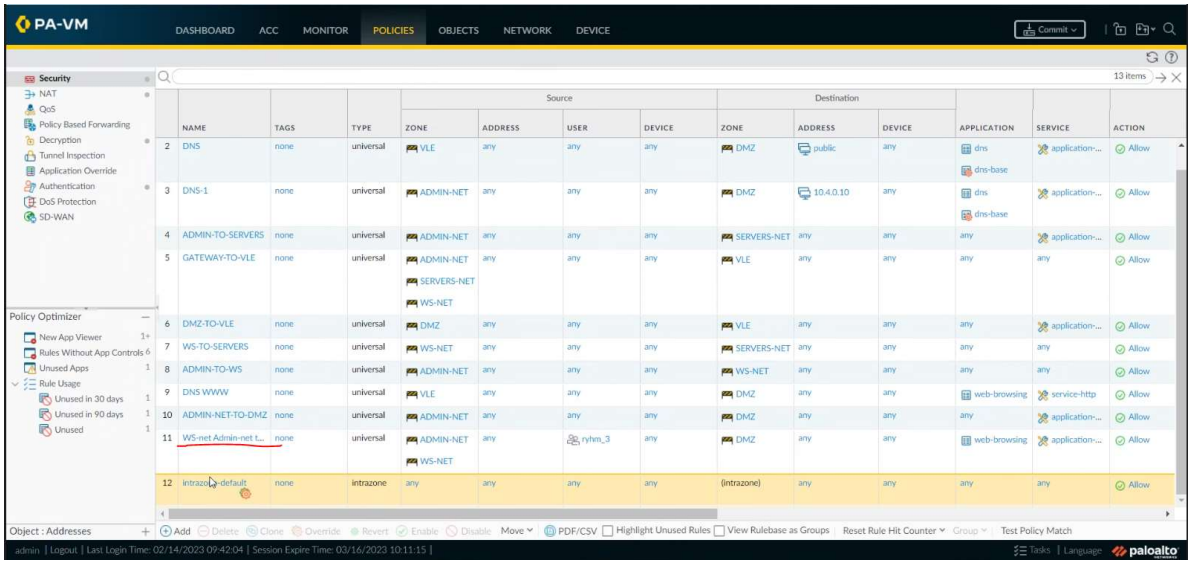


Kuva 5. Tunnistautumis tapa ryhm_3_captive_portal



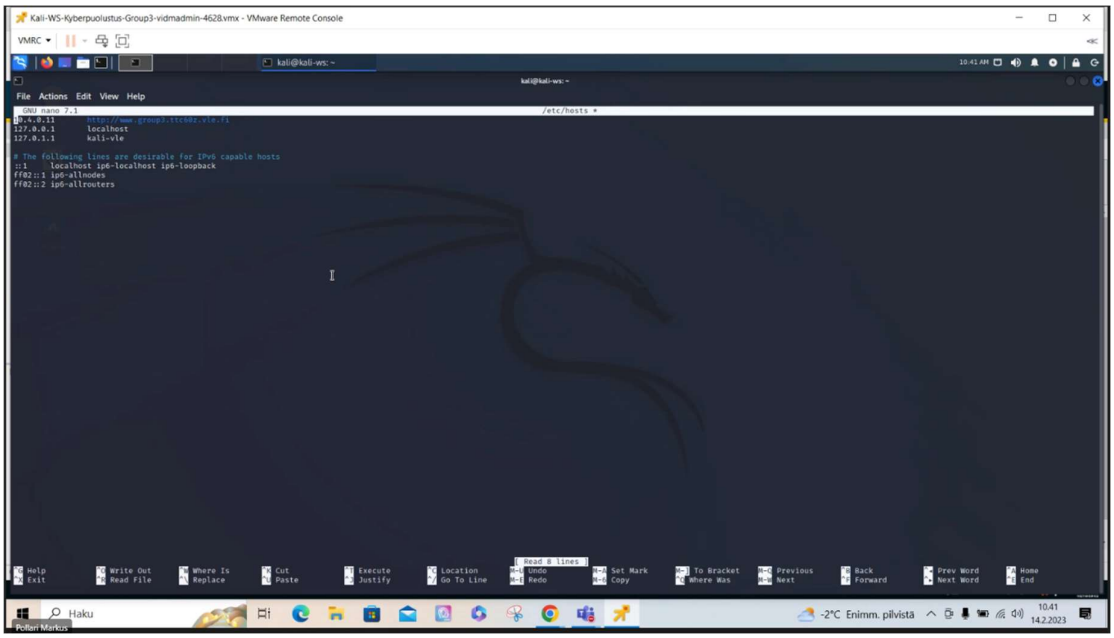
Kuva 6. Sääntö jolla vaaditaan tunnistautuminen

Luotiin uusi sääntö, jolla sallittiin liikenne WS ja Admin netistä DMZ:lle, sekä lisättiin source useriksi luomamme local user group. Esitetty kuvassa 7.



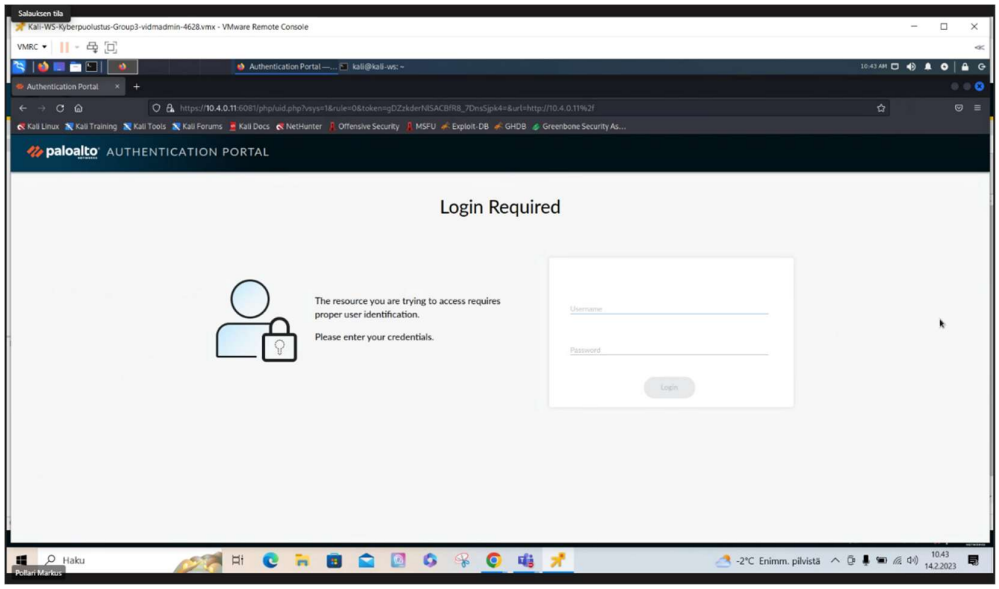
Kuva 7. Sallitu liikenne Admin- ja WS-netistä DMZ:lle

Käytiin kalilla ja ajettiin käsky sudo nano /etc/hosts, jota kautta päästiin muokkaamaan hosts tiedostoa lisäämällä sinne ympäristömme www palvelimen ip:n sekä sen osoitteen www.group3.ttc60z.vle.fi. Esitetty kuvassa 8.

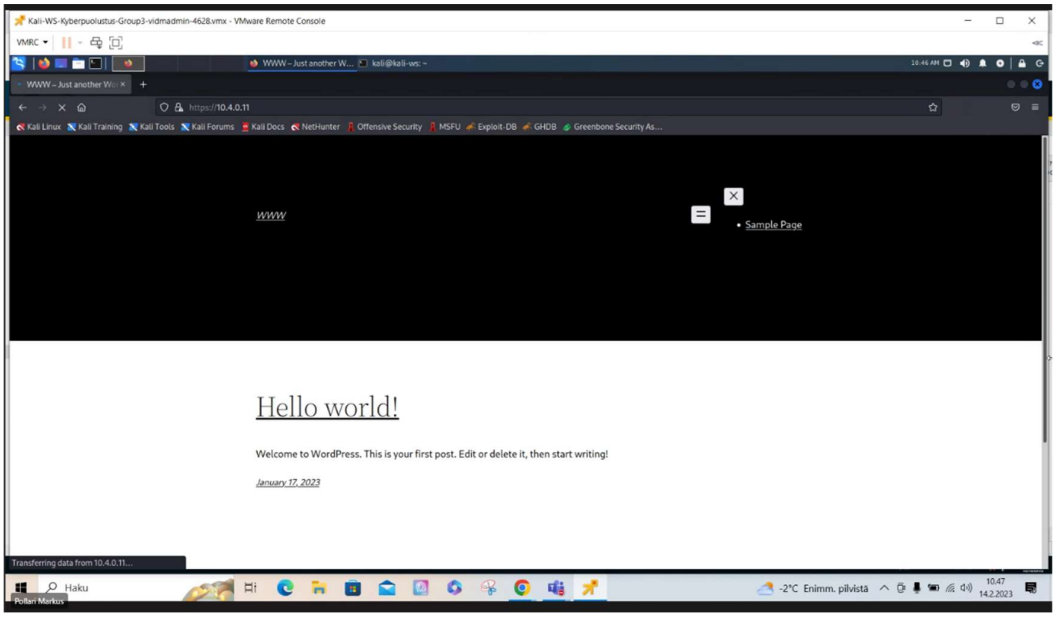


Kuva 8. Kali hosts tiedosto muokkaus

Mentiin kalilla www palvelimelle, josta huomattiin ensimmäisen kerran tunnistautumis säännön joka asetettiin kuvassa 6 toimivan. Tunnistautuminen onnisti luoduilla local usereilla ja päästiin sivustolle. Esitetty kuvissa 9 ja 10.

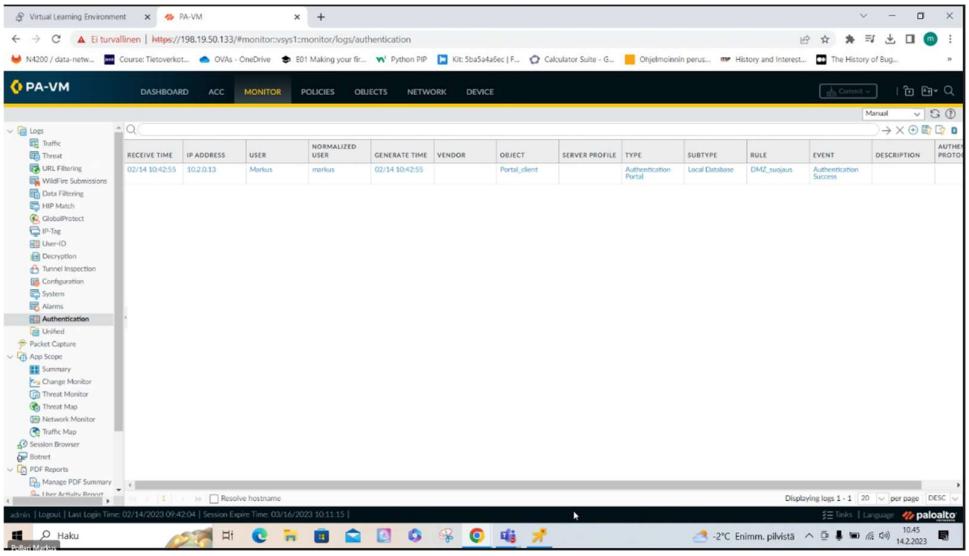


Kuva 9. Authentication



Kuva 10. Kalilla päästy onnistuneesti sivuille

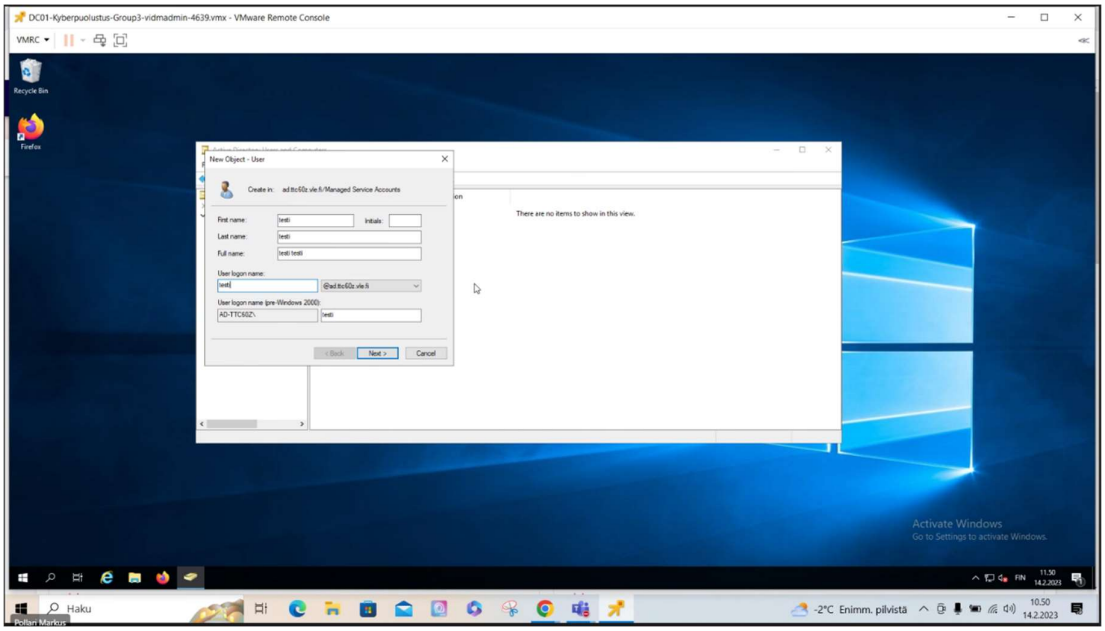
Paloaltosta nähtiin monitor authenticationissa onnistunut auhtentication joka tehtiin local tunnukella Markus. Esitetty kuvassa 11.



Kuva 11. Onnistunut authentication

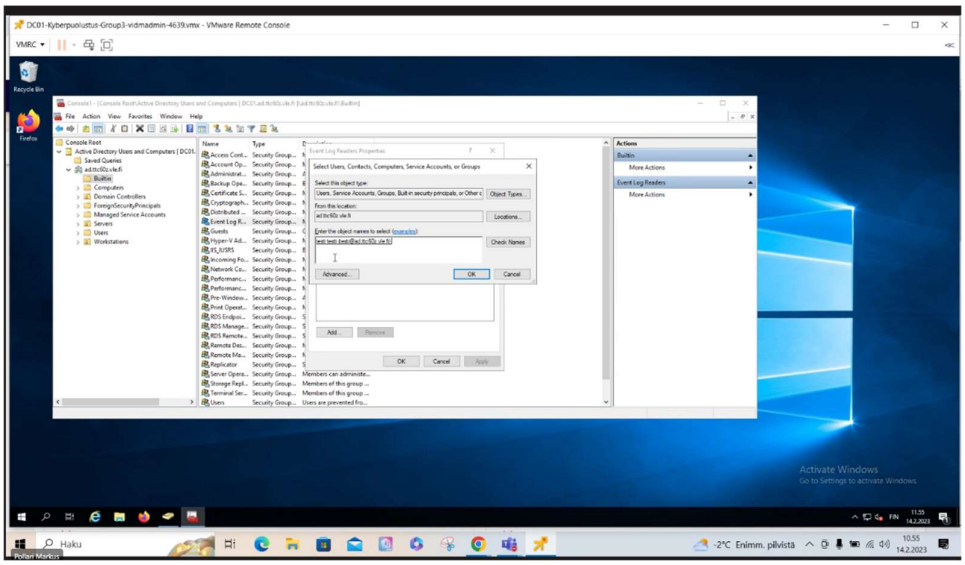
3.2 Paloalton integrointi AD:hen

Luotiin DC01 tietokoneelle User-ID agentille omistettu service account nimeltä testi. Esitetty kuvassa 12.



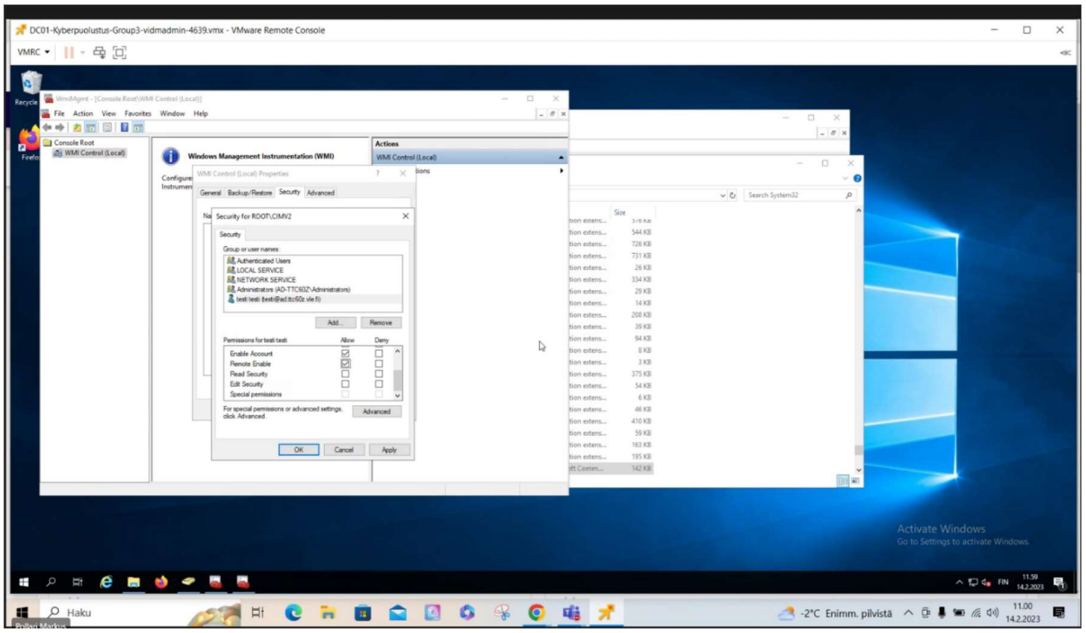
Kuva 12. Testi käyttäjä luonti

Määritettiin käyttäjien tunnistamista koskevat käyttöoikeudet luodulle testi käyttäjälle. Esitetty kuvassa 13.



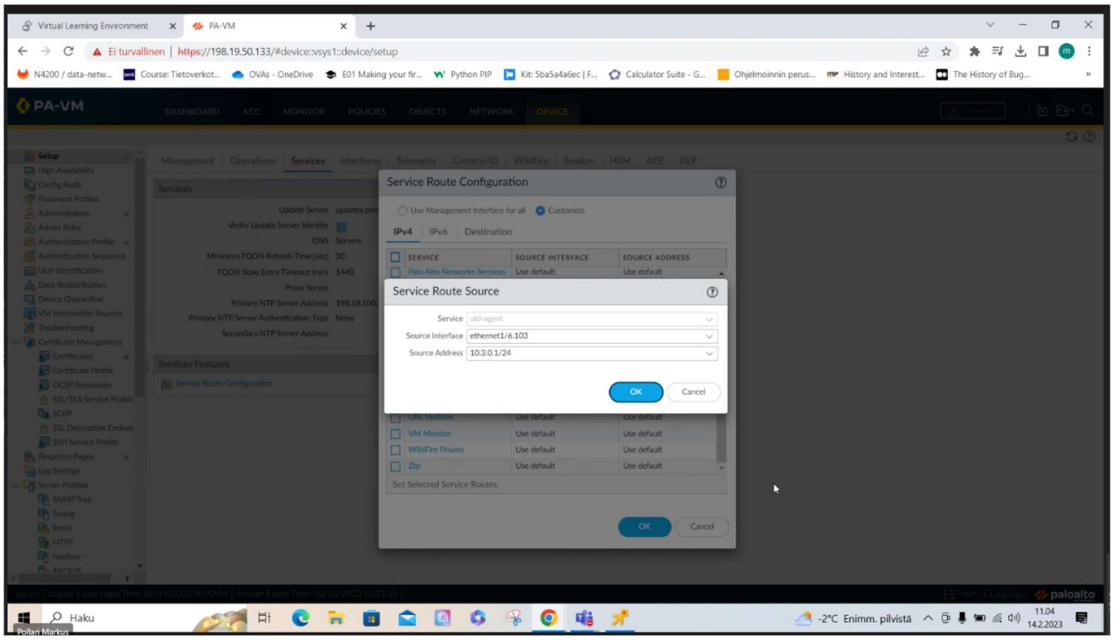
Kuva 13. Tunnistamista koskevat käyttöoikeudet.

Asetettiin testi service account lukemaan CIMV2 nimiavaruutta. Esitetty kuvassa 14.

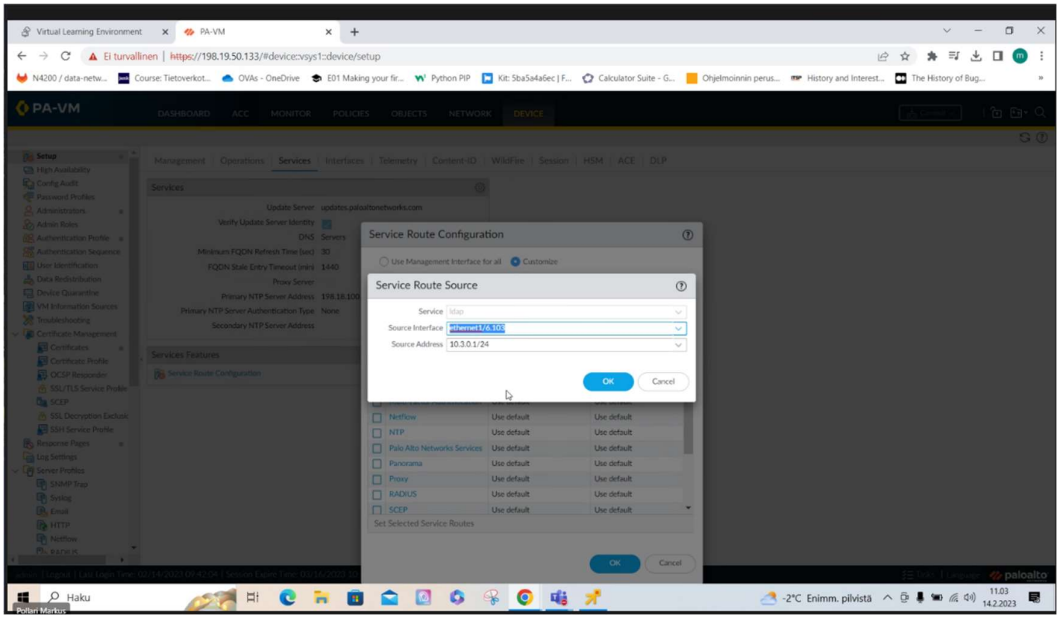


Kuva 14. CIMV2 asetus testi käyttäjälle

Vaihdettiin Service Route User-ID:lle, vaihdettiin LDAP ja UID agent source interface ethernet1/6.103. Esitetty kuvissa 15 ja 16.

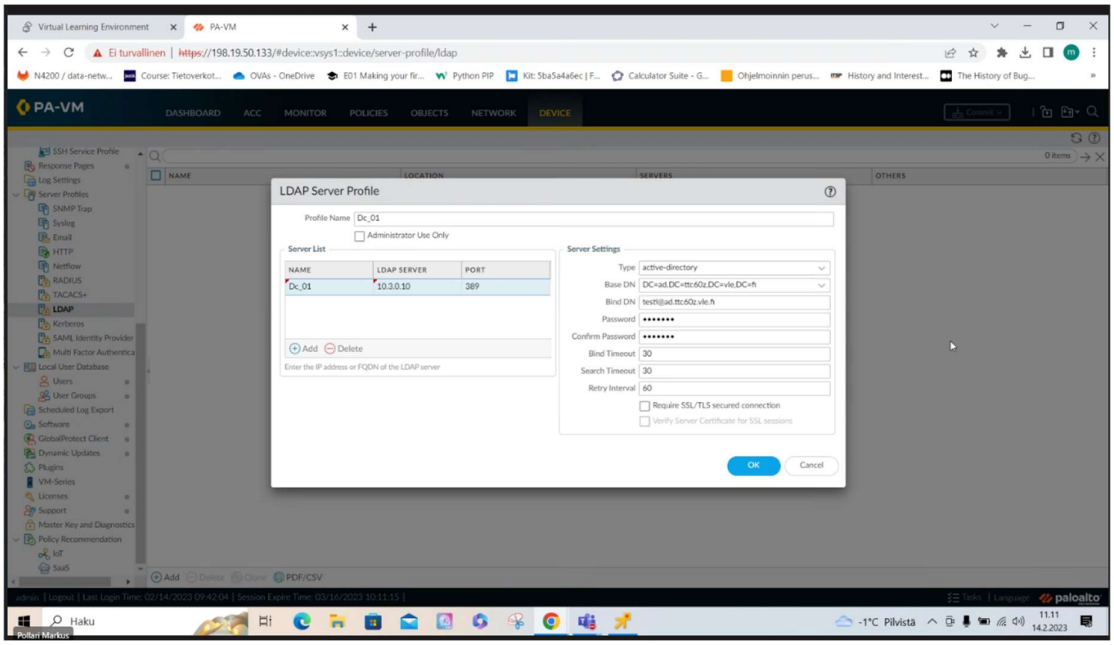


Kuva 15. UID Service route



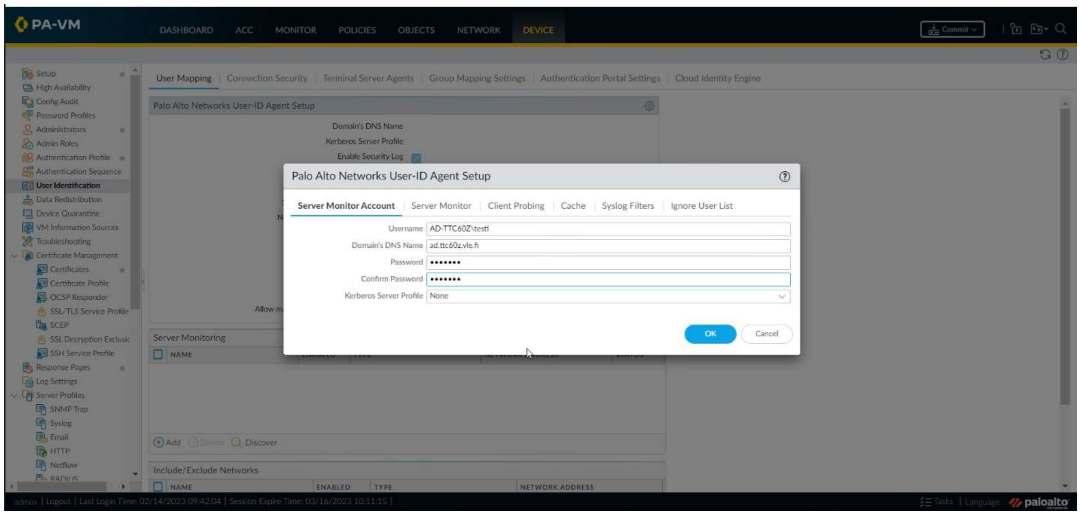
Kuva 16. LDAP Service route

Konfiguroitiin LDAP, luotiin uusi LDAP server jolle annettiin nimeksi Dc_01 sekä DC01 ip osoite 10.3.0.10. Server asetuksista lisättiin vielä tyypiksi active-directory, sekä BIND DN accounti testi@ad.ttc.60z.vle.fi. Asetettiin myös Require SSL/TLS secured connection unchecked. Esitetty kuvassa 17.



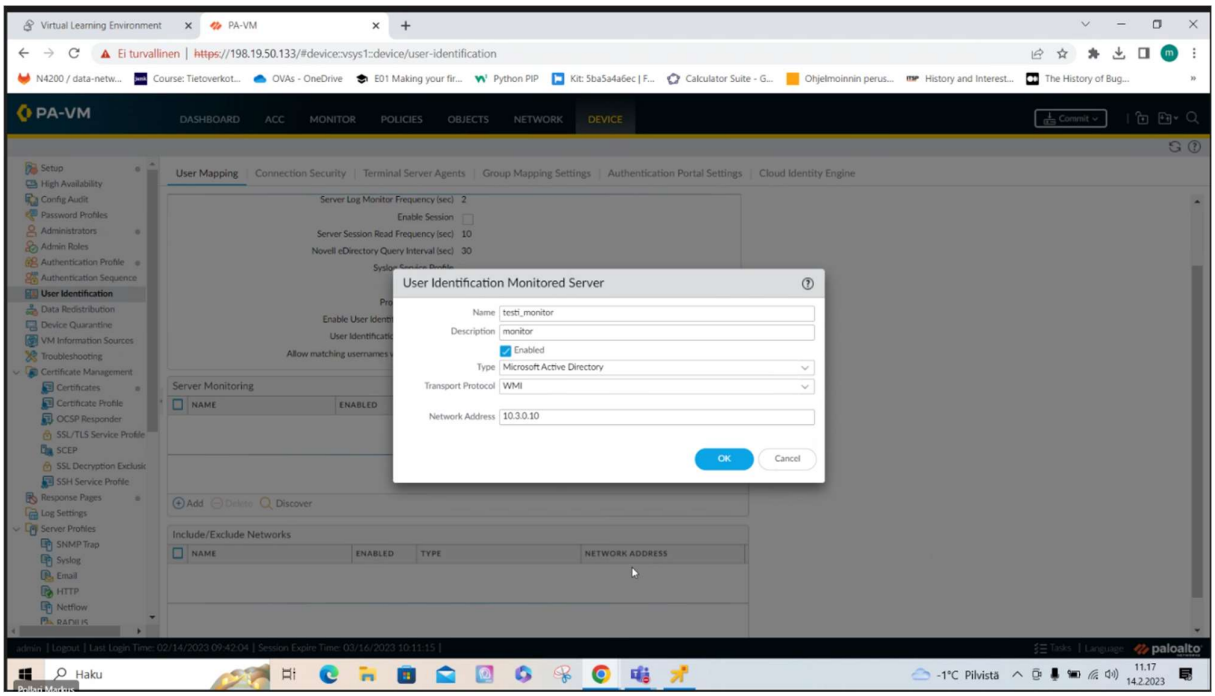
Kuva 17. LDAP konfiguraatio

User-ID Agent Setupista syötettiin service accountimme muodossa AD-TTC60Z\testi ja annettiin domainin DNS nimi ad.ttc60z.vle.fi sekä syötettiin testi käyttäjän salasana. Esitetty kuvassa 18.



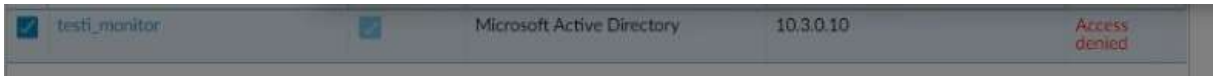
Kuva 18. User-ID Agent Setup.

Server monitoringiin syötimme nimen testi_monitor ja tyypiksi annettiin Microsoft Active Directory. Network addressiin syötimme DC01 ip osoitteen 10.3.0.10. Esitetty kuvassa 19.



Kuva 19. Server Monitoring settings.

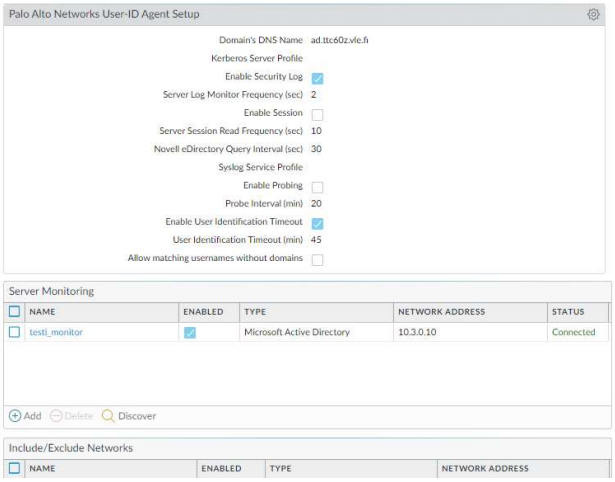
Tähän kohtaan jäimme jumiin pitkäksi aikaa, sillä emme saaneet luomaamme server monitoringiin yhteyttä, vaikka kävimme asetukset moneen kertaan läpi jopa opettajan kanssa. Esitetty kuvassa 20.



Kuva 20. Server monitoring Access denied.

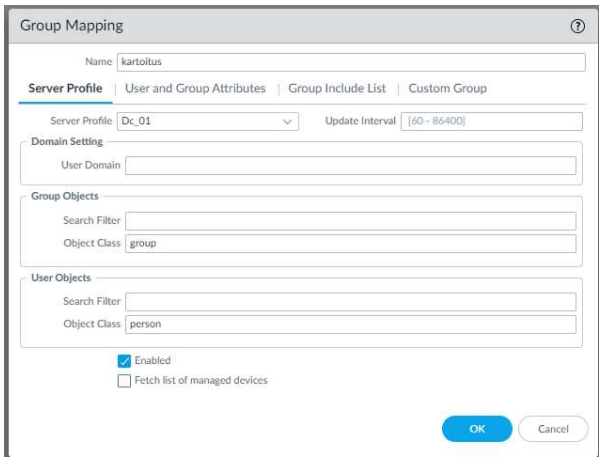
Testasimme monia eri korjauksia mitä netistä löysimme tähän ongelmaan liittyen. Tämän takia on vaikea sanoa mikä korjaus lopulta korjasi ongelmamme, sillä ongelma ratkesi ns. vähän yhtäkkiä hetken ajan päästä siitä, kun olimme erilaisia korjauksia testanneet. Esitetty kuvassa 21. Viimeisimmät korjaukset mitä paloaltossa kuitenkin teimme ennenkö, yhteys alkoi toimimaan, oli testi ser-

vice accountimme vaihto Administrator käyttäjään User-ID agent setupissa ja LDAP Server Profilessa. Nämä asetukset löytyvät kuvista 17 ja 18. Muutimme myös User Identification Monitored Server asetuksista Network addressin hetkellisesti muotoon dc01.ad.ttc60z.vle.fi joka antoi Acces denied sijaan Not connected, asetus on esitetty kuvassa 19. Vaihdoimme kuitenkin myöhemmin network addressin takaisin vanhaan IP osoitteeseen.

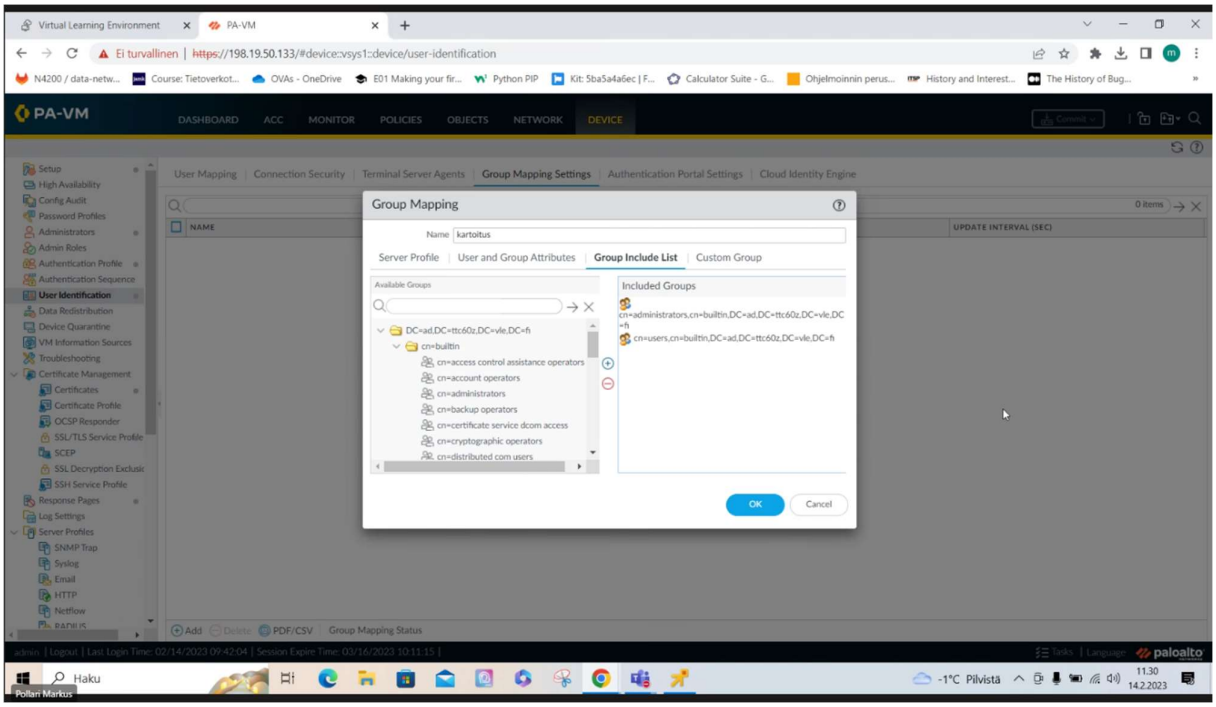


Kuva 21. Toimiva Server Monitoring yhteys.

Jotta pystymme lisäämään ryhmiä tehtyihin sääntöihimme tuli määrittää Group mapping. Nimeksi asetimme kartoitus ja server profiiliksi Dc_01. Group mappingiin annoimme ryhmät Administrators ja Users. Esitetty kuvissa 22 ja 23.



Kuva 22. Group mapping settings

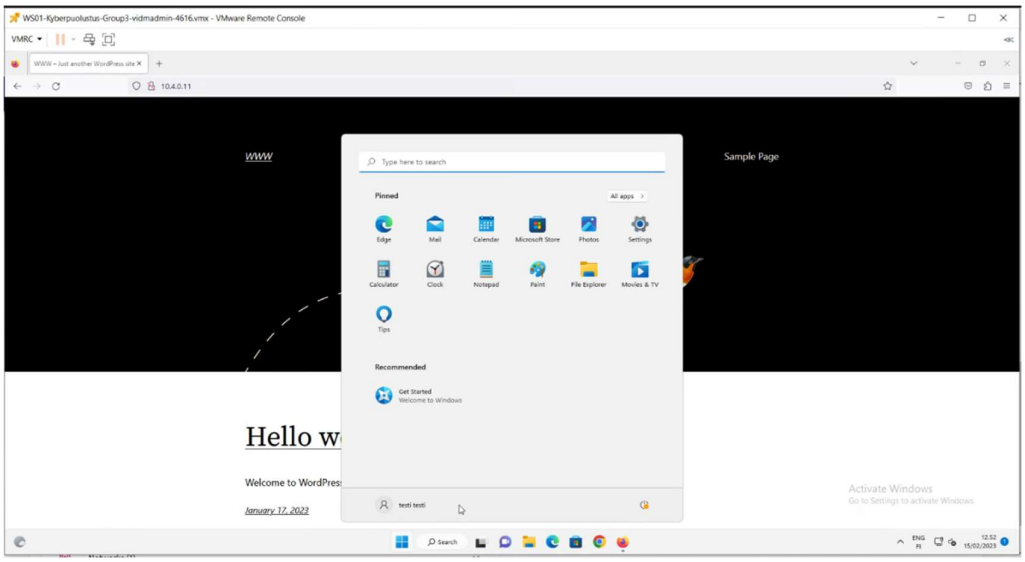


Kuva 23. Group mapping settings lisätyt ryhmät

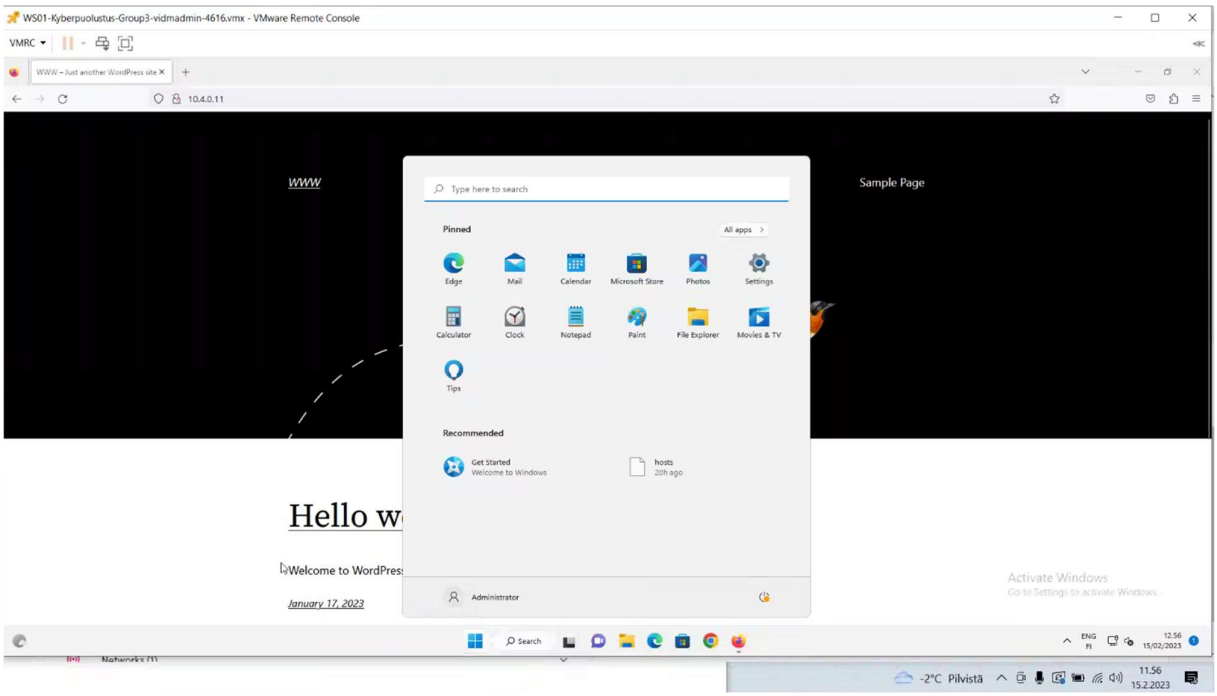
Nyt pystyimme lisäämään sääntöihin ryhmiä AD:sta. Lisäsimme AD:sta sääntöihin ryhmät Administrators ja users. Lisäsimme myös käyttäjän testi. Esitetty kuvassa 24.

Kuva 24. Sääntöihin lisätyt käyttäjät ja ryhmät

Nyt www palvelimet saatiin toimimaan myös lisätyillä AD-käyttäjillä. Esitetty kuvissa 25 ja 26.



Kuva 25. AD testi käyttäjä sivuilla



Kuva 26. Administrator käyttäjä sivuilla

4 POHDINTA

Neljänen laboratorioharjoituksen tarkoituksena oli tutustua User-ID:n hyödyntämiseen ja Captive portaliin. Harjoitustehtävän aikana ryhmä harjoitteli erilaisten käyttäjien ja ryhmien tunnistamista sekä sääntöjä, jota niille voidaan antaa, ja tätä kautta ryhmä tutustui user-ID:n sekä captive portalin käyttöön.

Harjoituksessa luotiin VLE ympäristön WWW palvelimelle tunnistautuminen niin, että vain tietyt käyttäjät pääsevät sisäverkosta www-sivuilemme. Tunnistautumiseen käytettiin harjoituksessa hyväksi paloaltossa toimivaa captive portalia. Tunnistautuminen tehtiin toimimaan Palo Altossa luoduilla local tunnuksilla, sekä ympäristön AD:ssa sijaitsevilla käyttäjillä. Dokumentaatiossa kerrottiin myös teoria User-ID:stä, Palo Alton Captive Portalista sekä LDAP:ista.

Harjoitustyö oli ohjeistettu hyvin esimerkkivideoilla, mutta kohtasimme harjoitustyötä tehdessä haasteen, johon jäimme jumiin pitkäksi aikaa. Kun kaikki tarvittavat toimenpiteet oli tehty ohjejeiden mukaan, emme silti saaneet luomaamme server monitoringiin yhteyttä (Access denied). Kävimme asetukset moneen kertaan läpi, myös opettajan kanssa. Testasimme monia eri korjauksia mitä netistä löysimme tähän ongelmaan liittyen. Vaikea sanoa mikä korjaus lopulta oli ratkaisu ongelmamme, sillä ongelma ratkesi ns. vähän yhtäkkiä hetken ajan päästä siitä, kun olimme erilaisia korjauksia testanneet.

Ongelmista huolimatta, harjoitustehtävä oli mielenkiintoinen ja kohtaamamme ongelman takia kävimme asetukset moneen kertaan läpi, joka auttoi ymmärtämään jokaisen kohdan tarkoituksen/tärkeyden syvemmin. Mietimme, että saiko “administrator” kirjoitusvirhe jotenkin sen rikki niin, että vaikka sen vaihtoi oikein, niin se ei silti pystynyt yhdistämään ennen kuin kaikki asetuksen oli kirjoitettu uudestaan, vaikka ne olivatkin oikein, jonka jälkeen se alkoi toimia. onko sääntöjen asettamisen/muuttamisen jälkeen aikaviive, joka vaikutti lopputulokseen. Teimmekö aluksi kaiken oikein, mutta säännöt eivät olleet tulleet voimaan vielä, kun niitä testasimme.

Ajallisesti harjoitustyö vei paljon aikaa ongelmatilanteen ratkaisemisen takia, mutta olimme tyytyväisiä opettajan intensiivisestä avusta, jota saimme kurssin viikko-ohjauksen aikana. Harjoitustyö kehitti ryhmätyöskentelytaitoja ongelmatilanteissa, joka on työelämässä tärkeä osa-alue hallita ja se kuuluu alalla työskentelemiseen.

Lähteet

Captive Portal Modes. 2023. Palo Alto Networks verkkosivut. Viitattu 17.2.2023. https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-admin/user-id/map-ip-addresses-to-users/map-ip-addresses-to-usernames-using-captive-portal/captive-portal-modes

Gillis, A.S. 12.2022. LDAP (Lightweight Directory Access Protocol). TechTarget verkkosivut. Viitattu 19.2.2023. https://www.techtarget.com/searchmobilecomputing/definition/LDAP

LDAP. 2023. Palo Alto Networks verkkosivut. Viitattu 19.2.2023. https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-admin/authentication/authentication-types/ldap#id9b2c506d-7319-4b39-894d-773ec210d587

User-ID N.d. Palo Alto Networks verkkosivut Viitattu 19.2.2023 https://www.paloaltonetworks.com/technologies/user-id