Veikko Henriksson

Tietokoneluokan koulutusympäristön kehittäminen ottamalla käyttöön Active Directory

Metropolia Ammattikorkeakoulu

Insinööri (AMK)

Tieto- ja viestintätekniikka

Insinöörityö

31.5.2022

Tiivistelmä

Tekijä:	Veikko Henriksson
Otsikko:	Tietokoneluokan koulutusympäristön kehittäminen ottamalla käyttöön Active Directory
Sivumäärä:	87 sivua + 3 liitettä
Aika:	31.05.2022
Tutkinto:	Insinööri (AMK)
Tutkinto-ohjelma:	Tieto- ja viestintätekniikan tutkinto-ohjelma
Ammatillinen pääaine:	IoT and Cloud Computing
Ohjaajat:	Osaamisaluepäällikkö Janne Salonen

Koulutusympäristön kehitystyö tehtiin Niemikotisäätiön Mieli Töihin -valmennusyksikössä Helsingissä. Mieli Töihin -valmennusyksikkö on erikoistunut tietotekniikkapainotteiseen valmennukseen, jonka tavoitteena on auttaa palveluiden käyttäjiä tieto- ja viestintätekniikkataitojen kohentamisessa sekä työllistymiseen ja opiskeluun liittyvissä asioissa.

Opinnäytetyön tarkoituksena oli kehittää tieto- ja viestintätekniikan lähiopetusympäristöä perinteisessä tietokoneluokkaympäristössä. Kehitystyön tarpeelle oli useita syitä. Aikaisempi koulutusympäristö muodostui lähiverkkoon kytketyistä yksittäisistä työasemista, joiden keskitetty hallinta oli vaillinainen. Tietoturvan ja tietosuojan kohentamisen vuoksi tarvittiin myös henkilökohtaiset käyttäjätunnukset kaikille käyttäjille ja opiskelijoille. Todettiin, että Microsoftin Active Directoryn käyttöönotto olisi luontainen valinta tietokoneluokkaan. Active Directorya ja palvelinympäristöä tarvittaisiin jatkossa myös oppimis- ja koulutustarkoitukseen, johtuen yksikössä suoritettavien TVT-perusopintojen ammattinäyttöjen vuoksi.

Opinnäytetyön keskiössä oli Active Directory, mutta raporttia kirjoittaessa sen ympärille alkoi kertymään palvelininfrastruktuuriin liittyviä muitakin oleellisia ja tärkeitä huomioitavia seikkoja. Raportissa kerrotaan palvelinalustan valinnasta sekä aihealueeseen liittyvistä tekniikoista ja vaihtoehdoista, kuten virtualisoinnista ja pilvilaskennasta. Neljännessä kappaleessa on joitakin huomioita myös tiedostojakoihin liittyen. Viidennessä kappaleessa käydään lävitse palvelimen tietoturvaan, etähallintaan ja varmistuksiin liittyviä asioita. En voinut jättää pois viimeistä kappaletta, joka liittyy ICT-palvelutuotannossa huomioitaviin ympäristöarvoihin. Hiilijalanjäljen minimointi ja kestävän kehityksen huomioiminen ICT-toimialalla tulee olemaan yksi tärkeimmistä arvostuksista ICT-palvelutuotannossa tulevaisuudessa.

Kehitystyö tehtiin suunnitelman mukaisesti syksyn 2021 aikana ja uusittu koulutusympäristö on tuotantokäytössä. Toimialueen jatkokehitysprojekti käynnistyy lähiaikoina.

Avainsanat: Aktiivihakemisto, Active Directory, Windows palvelin

Abstract

Author:	Veikko Henriksson
Title:	Developing a computer classroom training environment by deploying Active Directory
Number of Pages:	87 pages + 3 appendices
Date:	31.05.2022
Degree:	Bachelor of Engineering
Degree Programme:	Degree Programme in Information and Communication Technology
Professional Major:	IoT and Cloud Computing
Supervisors:	Janne Salonen, Principal Lecturer

The development of the educational environment work was carried out at the Mieli Töihin Training Unit of the Niemikotisäätiö in Helsinki. Mieli Töihin Coaching Unit specializes in information technology-focused coaching, which aims to help improve the use of ICT-skills in the use of services and in matters related to work and study.

The purpose of the thesis was to develop a contact teaching environment for information and communication technology in a traditional computer classroom environment. There were several reasons for the need for development work. The previous training environment consisted of individual workstations connected to the local network, the centralized management of which was incomplete. In order to increase data security and data protection, personal user IDs were also needed for all users and students. It was noted that the introduction of Microsoft Active Directory would be an inherent choice for the computer class. Active Directory and the server environment would also be needed in the future for learning and training purposes, due to the professional displays of basic ICT-studies in the unit.

At the heart of the thesis was Active Directory, but when writing the report, other important aspects related to the server infrastructure began to accumulate around it. The report describes the choice of server platform and related technologies and options, such as virtualization and cloud computing. The fourth paragraph also has some remarks regarding file sharing. The fifth section covers issues related to server security, remote management, and backups. I could not leave out the last paragraph, which relates to the environmental values to be taken into account in the production of ICT-services. Minimizing the carbon footprint and taking sustainable development into account in the ICT-industry will be one of the most important values in ICT-service production in the future.

The development work was carried out according to plan during the autumn of 2021 and the renovated training environment is in production use. The further development project of the domain will be launched shortly.

Keywords: Active Directory, Windows Server

Sisällys

Lyhenteet ja käsitteet

AAD	Azure Active Directory. Microsoftin pilvipalvelu, joka tarjoaa keskitettyä identiteetin ja käyttöoikeuksien hallintaa ulkoisille ja sisäisille resursseille.
AD	Active Directory. Microsoftin hakemistopalvelu eli aktiivihakemisto.
ADAC	Active Directory Administrative Center. Windows palvelimen hallintakeskus.
AD CS	Active Directory Certificate Services. Microsoftin Active Directoryn lisäpalvelu, joka perustuu varmenteisiin ja julkisen avaimen infrastruktuuriin.
AD DS	Active Directory Domain Service. Microsoftin hakemistopalvelu eli aktiivihakemiston peruspalvelut.
AD FS	Active Directory Federation Services. Microsoftin Aktiivihakemiston lisäpalvelu, joka tarjoaa kertakirjautumismahdollisuuden järjestelmiin ja sovelluksiin yli organisaatiorajojen.
AD LDS	Active Directory Lightweight Directory Services. Tarjoaa tuen hakemistokäyttöisille sovelluksille ilman Active Directoryn riippuvuuksia. Toimii erillisenä tietovarastona tai replikoinnin kanssa.
AD RMS	Active Directory Rights Management Services. Microsoftin palvelinohjelmisto, jonka avulla voi lisätä tietoturvaa liittyen asiakirjahallintaan organisaatiossa.

ADUC	Active Directory Users and Computers. Microsoftin hallintatyökalu Active Directorylle.
BIOS	Basic Input-Output System. Tietokoneen matalan tason tietokoneohjelma, joka ladataan tietokoneen käynnistyksessä. Ohjelma etsii ja lataa käyttöjärjestelmän keskusmuistiin.
CaaS	Container as a Service. Pilvipalvelutyyppi. Konttipohjainen virtualisointimalli, jossa tarjotaan säiliöitä suoraan verkosta. Käytetään esim. sovelluspaketoinnissa.
CAL	Client Access License. Käyttölisenssi palvelimelle. Laitteisto- tai käyttäjäpohjainen.
Cloud Computing	Pilvilaskenta. Tietokonejärjestelmän resurssien tarjoamista verkon kautta.
DaaS	Desktop as a Service. Pilvipalvelu, virtuaalinen työpöytä käyttäjälle. Tarkoittaa myös Data as a Service. Tällöin tarjotaan dataa pilvestä eri asiakkaan laitteille.
DC	Domain Controller eli toimialuepalvelin eli ohjainkone.
DFS	Distributed File System. Microsoftin hajautettu tiedostojärjestelmä.
DHCP	Dynamic Host Configuration Protocol. Verkkoprotokolla, jonka avulla jaetaan IP-osoitteita ja verkkoasetuksia automaattisesti asiakaskoneille.
DIT	Directory Information Tree. Hakemistotietopuu.
DN	Distinguished Names. Yksilöivä tunnistetieto LDAP-hakemistossa.

DNS	Domain Name System/Domain Name Services. Nimipalvelujärjestelmä/Nimipalvelin, joka muuntaa verkkotunnuksia IP-osoitteiksi ja toisin päin.
DSRM	Directory Services Restore Mode. Hakemistopalvelujen palautustila.
EMAS	The Eco-Management and Audit Scheme. Eurooppalainen ympäristöasioiden johtamisjärjestelmä.
Energy Star	Energiatehokkaiden tuotteiden kansainvälinen standardi.
ESE	Extensible Storage Engine. Microsoftin tiedontallennustekniikka.
FaaS	Function as a Service. Pilvipalvelu, toiminto palveluna.
FSMO	Flexible Single Master Operation. Isäntätoiminto, joita on viisi kappaletta aktiivihakemistossa.
FSRM	File Server Resource Manager. Windows palvelimen roolipohjainen lisäpalvelu tiedostojen hallintaan ja luokitteluun.
Global Catalog	Yleinen luettelopalvelu Active Directoryssa, joka tarjoaa tietoja koko metsän objekteista.
GP	Group Policy. Active Directoryn ryhmäkäytäntö.
GPO	Group Policy Object. Active Directoryn ryhmäkäytäntöobjekti.
GPResul.exe	Group Policy Result. Microsoftin komentorivityökalu ryhmäkäytäntöjen tarkasteluun työasemilla.

GPUpdate.exe	Group Policy Update. Microsoftin komentorivityökalu ryhmäkäytäntöjen asetuksien päivittämiseen.
GPU	Graphics Processing Unit. Grafiikkaprosessori.
GUID	Globally Unique Identifier. Maailmanlaajuinen yksilöllinen tunnistetieto hakemistopalvelussa.
Hardware	Tietokoneen laitteisto eli rauta.
Hot Plug	Laitteen kuuma kytkeminen mahdollista. Ei vaadi uudelleen käynnistystä esim. palvelimen kovalevyt.
Hypervisor	Ohjelmisto tai laitteisto. Luo ja käyttää virtuaalikonetta.
IaaS	Infrastructure as a Service. Pilvipalvelu, Infrastruktuuri palveluna.
IDaaS	Identity as a Service. Pilvipalvelu, todennus- ja identiteetinhallintapalvelu.
iDRAC7	Integrated Dell Remote Access Controller 7. Dellin palvelimiin upotettu hallintajärjestelmä.
IP-osoite	Internet Protocol -osoite. Yksilöivä laiteosoite internetissä.
IPv4	Internet Protocol version 4. Pakettivälitteisten verkkojen protokollan neljäs versio. 32-bittinen osoiteavaruus ja edelleen käytössä internetissä.
IPv6	Internet Protocol version 6. IPv4:n seuraaja, jossa osoiteavaruus on 128-bittinen.

IRM	Information Rights Management. Tietoturvateknologian muoto, käytetään suojaamaan arkaluontoisia tietoja sisältäviä asiakirjoja luvattomalta käytöltä.
ISAM	Indexed Sequential Access Method. IBM:n kehittämä tiedostonhallintajärjestelmä.
ISO 9001	Laatujärjestelmä. Kansainvälinen standardi.
ISO 14001	Ympäristöasioiden hallintajärjestelmä. Kansainvälinen standardi.
JET	Joint Engine Technology. Microsoftin kehittämä tietokantamoottori.
Kerberos	Kerberos on turvallinen todennusprotokolla, joka toimii tietokoneverkossa.
LDAP	Lightweight Directory Access Protocol. Hakemistopalvelujen käyttämä verkkoprotokolla.
LUT	Lappeenrannan-Lahden teknillinen yliopisto.
MMC	Microsoft Management Console. Microsoftin tarjoama graafinen hallintakonsolikehys järjestelmän hallintaan.
NetBIOS	Network Basic Input/Output System. Verkkotekniikan standardi (v.1983). Sallii sovellusten ja tietokoneiden kommunikoida lähiverkossa. Ei reititettävä protokolla.
NetBEUI	NetBIOS Extended User Interface. NetBIOS:n laajennettu versio.
NTFS	New Technology File System. Microsoftin kehittämä tiedostojärjestelmä.

NTDS.dit	Windows NT Directory Services. AD-palvelimen tietokantatiedosto.
NTLM	New Technology Lan Manager. MS Windowsin vanha turvaton autentikointiprotokolla.
NTP	Network Time Protocol. UDP-pohjainen protokolla aikatiedon välittämiseen.
OME	OpenManage Enterprise. Dellin infrastruktuurin hallintakonsoli.
OMSA	Open Manage Server Administrator. Dellin järjestelmänhallintaratkaisun ohjelmistoagentti.
OU	Organizational Unit. Organisaatioyksikkö. Objekti, jonka avulla voidaan ryhmittää objekteja hakemistopalvelussa eli Active Directoryssa.
OS	Operating System. Käyttöjärjestelmä.
OAuth	Open Authorization. Avoin standardi käyttöoikeuksien delegointiin internetissä.
PaaS	Platform as a Service. Pilvipalvelu, alusta palveluna.
PDC	Primary Domain Controller. Pääemulaattori. Yksi FSMO -rooleista aktiivihakemistossa.
Powershell	Microsoftin kehittämä monipuolinen komentorivitulkki komentojen ja skriptien ajoon.
RAID	Redundant Array of Independent Disks. Tietokoneiden vikasietoisuutta tai nopeutta lisäävä tekniikka, jossa käytetään useita kiintolevyjä.

RAM	Random Access Memory. Tietokoneen keskusmuisti.
RDC	Remote Desktop Connection. Microsoftin etähallinta-ohjelma.
RDN	Relative Distinguished Name. Yksilöivän tunnistetiedon suhteellinen viittaustieto.
RDP	Remote Desktop Protocol. Microsoftin graafinen etähallintaprotokolla.
RID	Relative Identifier. Yksi FSMO-rooleista aktiivihakemistossa.
RSAT	Remote Server Administration Tools. Palvelimien etähallintatyökalut työasemille.
RSoP	Resultant Set of Policy. Microsoftin työkalu ryhmäkäytäntöjen tarkasteluun työasemilla.
Ryhmäkäytäntö	Group Policy. Sääntö, jolla voidaan hallita tietokoneiden ja käyttäjien asetuksia.
SaaS	Software as a Service. Pilvipalvelu, ohjelmisto palveluna.
SAML	Security Assertion Markup Language. XML-standardi tietojärjestelmien käyttäjien tunnistamiseen ja valtuuttamiseen.
SAP	Systeme, Anwendungen und Produkte in der Datenverarbeitung. Saksalainen ohjelmistovalmistaja. Yritys on erikoistunut mm. toiminnanohjausjärjestelmiin.
SAS	Serial Attached SCSI. Sarjamuotoinen tietokoneväylä.

Schema	Kaava. Sisältää kaikki muodolliset määrittelyt Active Directoryn koko metsän alueella.
SID	Security Identifier. Yksilöllinen suojaustunniste, jota hakemistopalvelu käyttää.
SLA	Service Level Agreement. Palvelutasosopimus.
SMB	Server Message Block. IBM:n ja Microsoftin kehittämä suosittu viestintäprotokolla verkossa.
SSD	Solid State Drive. Tietokoneen massamuisti, jossa ei liikkuvia osia.
SSO	Single Sign-On. Kertakirjautuminen.
TCO	Total Cost of Ownership. Kansainvälinen kestävän kehityksen sertifikaatti IT-tuotteille.
TCP	Transmission Control Protocol. Yhteydellinen ja luotettava tietoliikenneprotokolla.
TIEKE	Tietoyhteiskunnan kehittämiskeskus.
TIVIA	Tieto- ja viestintätekniikan ammattilaiset. Valtakunnallinen tietotekniikka-alan yhdistysten yhteistyöjärjestö.
Toimialue	Domain. Active Directoryn looginen ryhmä objekteja, joilla on yhteiset hallinta-, suojaus- ja replikointiasetukset.
Toimialuemetsä	Domain Forest. Active Directoryn kokoelma toimialuepuita.

Toimialuepuu	Domain Tree. Toimialueen ja alitoimialueiden muodostama kokonaisuus, joilla on yhteinen kaava.
UDP	User Data Protocol. Yhteydetön tietoliikenneprotokolla.
UPN	User Principal Name. Active Directoryn yksilöllinen kirjautumisnimi, joka on sähköpostimuotoinen.
UPS	Uninterruptible Power Supply. Keskeytymätön virran syöttölaite tai järjestelmä, joka suojaa lyhyissä sähkökatkoksissa tietokoneita, etenkin palvelimia. Suodattaa myös sähkönsyötön. Sisältää akuston.
VBS-skripti	Visual Basic Script. Microsoftin ohjelmointikieli.
VMM	Virtual Machine Monitor. Virtuaalikonemonitori. Kts. Hypervisor.
VSS	Volume Shadow Copy Service. Levyaseman tilannevedospalvelu.
XaaS	Anything as a Service. Pilvipalvelu, X voi olla mikä tahansa palvelu.
Zenmap	Avoimeen lähdekoodiin perustuva Ilmainen ja graafinen verkon skannausohjelma.

1 Johdanto

Työn tarkoituksena on kehittää tieto- ja viestintätekniikan lähiopetusympäristöä perinteisessä tietokoneluokkaympäristössä. Kehitysprojektin aikana on tarkoitus samalla tutustuttaa Tieto- ja viestintätekniikan perustutkintoa opiskelevia oppilaita palvelinympäristöihin. Kehitystyö tehdään syksyn 2021 aikana Niemikotisäätiön Mieli Töihin -valmennusyksikössä Helsingissä.

Työn keskiössä on Microsoftin Active Directory ja siihen liittyvät tarvittavat peruspalvelut. Työssä käsitellään myös muita palvelininfrastruktuuriin liittyviä seikkoja, jotka ovat työn kannalta oleellisia. Lähestymistapa on käytännönläheinen ja työssä esitellään yleisimpiä huomioitavia seikkoja liittyen palvelininfrastruktuuriin. Palvelinalustana (hardware) käytetään perinteistä tornimallista ”rautapalvelinta”.

Työn aihepiiri on melko laaja, koska työn tarkoituksena on myös tutustua palvelininfrastruktuuriin oppimis- ja opetustarkoituksessa. Työraportissa käsitellään joitakin palvelininfraan liittyviä seikkoja vain pintapuolisesti, koska muuten työselosteesta muodostuisi liian pitkä. Internetistä löytyy runsaasti lähdemateriaalia aiheiseen liittyen esimerkiksi videomuodossa, mikä lienee nykyisin nopein tapa hankkia lisätietoa. Microsoftin verkossa olevat dokumentaatiot ja perinteiset opukset kirjastosta ovat luonnollisesti myös erinomaisia tietolähteitä.

1.1 Aikaisempi tietokoneluokkaympäristö

Aikaisempi kehitettävä tietokoneluokan koulutusympäristö muodostuu kymmenestä paikallisesta Windows-työasemasta, jotka ovat kytketty lähiverkkoon, jonka kautta tarjotaan internet-yhteys. Työasemiin kirjaudutaan yhteisellä paikallisella tunnuksella, joko automaattisesti tai manuaalisesti. Opiskelijat käyttävät yhteistä tunnusta, jolloin työasemien puhdistus edellisten käyttäjien tiedostoista joudutaan tekemään aina kurssien jälkeen manuaalisesti. Tietosuojan ylläpito on haasteellista, koska kurssin aikana toinen opiskelija tai käyttäjä pystyy käyttämään samaa

konetta yhteisellä tunnuksella opintojaksojen välissä. Työasemissa on paikallinen järjestelmänvalvoja-tunnus ylläpitotehtäviä varten erikseen.

Koulutusmateriaali jaetaan vanhanaikaisesti USB-tikuilla ja harjoitustyöt tallennetaan USB-tikuille tai paikalliseen kansioon työasemalle. Kouluttajalla ei ole pääsyä työasemille verkon kautta ja ohjelmistoasennukset ja päivitykset tehdään pääosin paikallisesti.

Virussuojausohjelmisto työasemilla on keskitetty ratkaisu, jota mikrotuki hallinnoi. Mikrotuki hallinnoi työasemia lisäksi kolmannen osapuolen hallintatyökalulla, mutta se ei kata kaikkia ohjelmia eikä käyttöjärjestelmään liittyviä asetuksia voida tehdä keskitetysti.

1.2 Tuleva tietokoneluokkaympäristö

Ottamalla käyttöön Microsoftin tarjoama paikallinen hakemistopalvelu eli Active Directory koulutusympäristössä, saadaan monia hyödyllisiä asioita, jotka helpottavat työasemien hallintaa ja käyttöä. Kouluttajan on tällöin myös helpompi hallita ja jakaa opetusmateriaalia verkkokansioiden avulla. Opiskelijat voivat tallentaa tehdyt harjoitustehtävät omiin kotikansioihinsa verkossa. Kouluttaja pääse helposti verkon kautta tarvittaessa tarkistamaan palautetut tehtävät kotikansioista. USB-tikkuja ei välttämättä tarvita lainkaan, ellei haluta opettaa niiden käyttöä yleisellä tasolla. Henkilökohtaisten tunnuksien myötä tietoturva ja tietosuoja kohentuu sekä tiettyjä koulutusmateriaaleja voidaan kohdentaen jakaa eri oppilasryhmille.

Kurssien tai harjoittelujaksojen välillä ei tarvitse manuaalisesti puhdistaa koneita edellisten opiskelijoiden jäljiltä, vaan käyttäjätunnuksen ja profiilin voi joko poistaa tai ottaa pois käytöstä kurssin tai jakson jälkeen. Tämän lisäksi tarkoituksen on hyödyntää keskitettyä hallintamahdollisuutta Active Directoryssa mm. ryhmäkäytäntöjen avulla. Autenttista toimialuemallia voidaan käyttää myös TVT-perusopiskelijoiden perehdyttämiseen aihealueeseen.

Aluksi työssä otetaan vain yksi toimialueen ohjauskone käyttöön, mutta mahdollisesti myöhemmin hankitaan toinen palvelin. Suunniteltu ratkaisu on kuitenkin riittävän vikasietoinen, koska paikalliset varatunnukset työasemilla pidetään käytössä. Tämä mahdollistaa käyttö- ja opetusympäristön toimimisen myös palvelimen mahdollisessa vikatilanteessa, jolloin kirjautuminen työasemille paikallisella tunnuksella on edelleen mahdollista. Tarvittaessa hätätapauksessa myös koulutusmateriaalin jakaminen onnistuu edelleen myös USB-tikuilla, vaikka Active Directory -palvelin ja siinä olevat tiedostojaot olisivat jostain syystä saavuttamattomissa. Tämän lisäksi varmuuskopioita tehdään päivittäin käyttäjien työtiedostoista keskitetysti, jolloin tärkeitä tietoja ei häviä, vaikka palvelimen kaikki kiintolevyt rikkoontuisivat yhtäaikaisesti.

1.3 Projektin vaiheet

Koulutusympäristön tekninen kehitystyö toteutettiin Niemikotisäätiön Mieli Töihin -yksikössä syksyn 2021 aikana tuotannon pyöriessä samanaikaisesti. Budjetti oli kohtuullisen kevyt, koska käytimme vanhaa palvelinta alustana. Palvelinrauta päivitettiin kiintolevyjen osalta nykyaikaan. Käytimme niin ikään saatavilla olevia ohjelmistolisenssejä, joten niihin ei myöskään tarvinnut investoida. Mikrotuen varastosta löytyivät lisäksi kaikki tarvittavat työvälineet ja apumuistit. Henkilöresurssina toimi tietotekniikkakouluttajan työpanos oman toimen ohella. Työvaiheet pääpiirteittäin olivat:

- Kehitystarpeen toteaminen, päätös ja tavoite.
- Suunnitelma, budjetti, aikataulutus ja resurssit.
- TVT-perusopiskelijoille luennot aiheesta projektin aikana.
- Palvelinalustan (palvelimen) hankinta, työvälineet, vaihtokomponentit ja ohjelmistolisenssit.
  - (a) Palvelimen fyysinen asennus (hardware).
  - (b) RAID1-levyjärjestelmän käyttöönotto.
  - (c) Käyttöjärjestelmän asennus, päivitys, tarkistus ja testaus.
  - (d) Verkkoasetukset (staattinen osoite) verkkotestaus.
  - (e) Active Directoryn asennus ja käyttöönotto.
  - (f) Verkkomäärittelyt (DNS-asetukset).

(g) Aika-asetuksien konfigurointi ja synkronointi palvelimeen.
(h) Palvelimen tietoturva- ja terveystarkistus sekä ns. ”parhaat käytännöt”.
(i) Etähallintatyökalujen käyttöönotto.

- Active Directoryn hallintamallin luonti, ryhmät ja käyttäjätunnukset.
- Työasemien kytkeminen vaiheittain toimialueeseen ja testausjakso.
- File Server Resource Manager (FSRM) -palvelun asennus.
- Kansiojaot, käyttöoikeudet ja kansioiden linkitykset.
- Ryhmäkäytännöt ja niiden testaus.
- Varmistuksien suunnittelu ja toteutus.
- Päivityksien automatisointi.
- Työasemien virransäästöasetukset ja huoltoikkunan määrittelyt.
- Tekninen osuus kehitysprojektista päättyi.
- Seuranta ja tuotantokäyttö alkoi.
- Palvelimen normaali hallinta- ja ylläpitotyö jatkumona.
- Koulutus ja opastus.
- Jatkokehitystyö aloitetaan suunnitellusti v. 2022 syksyllä.

2 Niemikotisäätiö ja Mieli Töihin -valmennusyksikkö

Niemikotisäätiö

Vuonna 1983 perustettu **Niemikotisäätiö** toteuttaa sääntöjensä mukaan sosiaalipsykiatrista kuntoutustyötä ja ehkäisevää mielenterveystyötä helsinkiläisille avohoidossa oleville mielenterveyskuntoutujille. Säätiö on vuodesta 2011 lähtien ollut Helsingin kaupungin tytäryhteisö, osa kaupunkikonsernia. Niemikotisäätiö toimii yleishyödyllisiä periaatteita noudattaen ja säätiön tarkoituksena ei ole tuottaa voittoa.

Niemikotisäätiö on mukana helsinkiläisten mielenterveyskuntoutujien elämässä. Niemikotisäätiö järjestää asumista, työtä, koulutusta, valmennusta, opiskeluita ja päivä- ja vapaa-ajantoimintaa. Palvelut tarjoavat selkeän kokonaisuuden, jotka tukevat palvelunkäyttäjiä heidän elämänsä eri vaiheissa. Toiminta perustuu toipumisorientaatioon (”Recovery-malli”). Tämän toimintafilosofian mukaisesti

palveluidenkäyttäjien itsenäinen päätöksenteko, oma kokemus, omat tavoitteet ja toiveet ovat keskeisellä sijalla toipumisessa. [1]

Mieli Töihin -valmennusyksikkö

TVT-koulutusympäristön kehitystyö tehtiin **Niemikotisäätiön Mieli Töihin -valmennusyksikössä**. Yksikkö sijaitsee Helsingissä ja se on erikoistunut tietotekniikkapainotteiseen valmennukseen, jonka tavoitteena on auttaa palveluiden käyttäjiä tieto- ja viestintätekniikkataitojen kohentamisessa sekä työllistymiseen ja opiskeluun liittyvissä asioissa. Opiskelu Mieli Töihin -valmennusyksikössä toteutetaan oman jaksamisen mukaan tekemällä oppien. Toiminta on digiosallisuutta, opiskelu- ja työelämävalmiuksia edistävää sosiaalista kuntoutusta.

Yksikössä voi laaja-alaisesti opiskella TVT-tekniikan eri osa-alueita. Opiskella voi ajoittain tai tarpeen mukaan järjestettävillä kursseilla tai omien intressien mukaisilla räätälöidyillä opiskelujaksoilla. Yksikkö tarjoaa kävijöille myös mahdollisuuden suorittaa Tietoyhteiskunnan kehittämiskeskus ry (TIEKE) @-kortin (4,5 op) ja/tai Tietokoneen käyttäjän A-kortin (7,5 op). Yksikössä voi opiskella ja suorittaa TVT-perustutkinnon (ent. datanomin tutkinto) ammattinäytöt (käytön tuki). Tämän lisäksi toimintayksikkö tarjoaa tietoteknistä tukea asiakkaiden omien laitteiden hankinnassa, käyttöönotossa, ylläpidossa ja huolloissa. Yksikössä toimii myös Niemikotisäätiön mikrotukipalvelu.

3 Active Directory (AD) ja palvelininfrastruktuuri

Active Directory (AD) on Microsoftin vuonna 2000 julkaisema hakemistopalveluratkaisu eri kokoisille organisaatioille maailmanlaajuisesti. Palvelu sisältyy Windows Server -konseptiin ja on otettavissa käyttöön tarvittaessa. Hakemistopalvelimen hajautettu tietokanta sisältää tietoa käyttäjistä, ryhmistä, tietokoneista, sovelluksista ja verkon resursseista. Se on verkkokäyttöjärjestelmä, joka mahdollistaa tietoturvallisen resurssien jakamisen käyttäjille ja sovelluksille. Se tarjoaa järjestelmän pääkäyttäjille ja ylläpitäjille tavan nimetä, kuvata, paikallistaa, hallita ja suojata käytössä olevia verkon resursseja.

Active Directorya käytetään usein puhtaassa Windows-laiteympäristössä, mutta se tukee myös Linux- ja Mac-ympäristöä. Active Directoryn liikennöintiprotokollina on Lightweight Directory Access Protocol (LDAP) ja Kerberos (autentikaatioprotokolla). Tässä kehitysprojektissa ei asenneta koko organisaation kattavaa ratkaisua, vaan kysymys on paikallisesta ratkaisusta tietokoneluokkaan. [2]

Organisaatiot käyttävät Active Directorya ensisijaisesti todennukseen ja valtuutukseen. Organisaation pääkäyttäjät voivat hallita keskitetysti hajautettua tietojärjestelmää erilaisilla työkaluilla loogisesti ja tehokkaasti. Organisaation oman Active Directory -hakemistopalvelun voi tarvittaessa integroida tai synkronoida Microsoftin tarjoamiin pilvessä toimiviin palveluihin, kuten Azure Active Directoryyn (AAD) ja sen kautta Office365 -pilvipalveluihin. Microsoftin Azure Active Directory -pilvipalvelu tarjoaa myös mobiililaitteille (Android ja IOS) keskitettyä hallintaa. [3]

3.1 Active Directoryn peruskäsitteitä

Active Directoryssa tiedot järjestetään puumaiseen LDAP-hakemistoon. Se on hierarkkinen malli, jota kutsutaan Directory Information Tree (DIT) -malliksi. Tietokantatiedoston nimi on NTDS.dit ja se sijaitsee AD-palvelimen systeemilevyllä omassa kansiossaan (kohdassa 3.1.3 kerrotaan tarkemmin tietokannasta).

Hakemistopalvelussa eli Active Directoryssa on objekteja ja ne jakaantuvat säiliöihin (containers) ja ei-säiliöihin (non-containers). Ei-säiliöitä kutsutaan myös lehtisolmuiksi (leaf nodes). Säiliöt voivat sisältää muita säiliöitä tai lehtisolmuja. Ei-säiliöt eli lehtisolmut eivät voi sisältää muita säiliöitä.

Schema

Active Directoryn Schema eli kaava sisältää kaikki muodolliset määrittelyt objektiluokille ja niiden attribuuteille aktiivihakemistossa koko metsän alueella.

Globally Unique Identifier (GUID)

Kaikilla objekteilla Active Directoryssa on yksilölliset tunnisteet eli GUID:it (Globally Unique Identifier). Kun esimerkiksi uusi toimialueen käyttäjä- tai ryhmätili luodaan, niin AD tallentaa tilin SID:n (Security Identifier) käyttäjä- tai ryhmäobjektin Object-SID (ObjectSID) -ominaisuuteen. Samassa yhteydessä määritetään uudelle objektille maailmanlaajuinen 128-bittinen yksilöllinen tunniste eli GUID. GUID-tunniste on tallennettu objektin Object-GUID (ObjectGUID) -ominaisuuteen. Active Directory käyttää sisäisesti GUID-tunnisteita objektien tunnistamiseen. GUID ei koskaan muutu, vaan se säilyttää tämän arvon siihen asti, kunnes objekti poistetaan AD:stä. GUID (ObjectGUID) julkaistaan AD:n yleisessä luettelopalvelussa eli Global Catalog -palvelussa, jolloin objekti on löydettävissä. Global Catalog -palvelu esitellään tarkemmin kohdassa Global Catalog (yleinen hakupalvelu) sivulla 10. [4, s.31-33].

Distinguished Names (DN)

Objekteilla on GUID-tunnisteen lisäksi käytössä yksiselitteinen Distinguished Names (DN) tunnistetieto, jota käytetään yksilöimään objekteja LDAP-hakemistossa. LDAP-protokolla määrittelee tämän hakemiston objekteihin liittyvän viittaustavan syntaksin ja säännöt. Yksiselitteiset tunnistetiedot (DN) luodaan käyttämällä kolmen tyyppisiä nimeämisattribuutteja:

- organizationName (O) tai organizationalUnitName (OU)
- domainComponent (DC)
- commonName (CN).

Relative Distinguished Name (RDN) avulla voidaan viitata objektiin, joka on ko. säiliön sisällä. Se on suhteellinen viittaustapa ja jos objektin sijainti muuttuu hierarkiassa, niin nimikin muuttuu. Saman säiliön sisällä ei voi olla muita objekteja samalla RDN-tunnistetiedoilla. Toisaalta eri säiliössä olevilla objekteilla voi olla sama RDN-tunnistetieto. [4, s. 33-34]

3.1.1 Active Directoryn looginen rakenne ja yleinen hakupalvelu

Active Directoryn loogisia rakenteita ovat:

- organisaatioyksikkö (OU, Organizational Unit)
- toimialue (Domain)
- toimialuepuu (Domain Tree)
- toimialuemetsä (Domain Forest).

Organisaatioyksikkö

Organisaatioyksikkö (OU) on hallintamallin oleellisin ja hyödyllisin taso käytännön kannalta. Niistä muodostettu rakenne perustuu yrityksen tarpeisiin ja noudattelee usein yrityksen todellista organisaatiorakennetta. Siihen voidaan sijoittaa ryhmiä, käyttäjiä ja tietokoneita. Organisaatioyksikön alle voi sijoittaa myös toisia organisaatioyksiköitä. Active Directoryn hierarkkinen hallintamallin rakentaminen esitetään myöhemmin kohdassa 4 sivulla 32.

Toimialue

Toimialue on Active Directoryn perusyksikkö, joka rakentuu loogisesta ryhmästä objekteja, joilla on yhteiset hallinta-, suojaus- ja replikointiasetukset. Toimialue muodostaa yhteisen hallinnollisen alueen hallita laitteita, käyttäjiä, resursseja, palveluita ja järjestelmiä keskitetysti. Toimialueen nimi tulee olla yksilöllinen ja toimialueen nimi pitää rekisteröidä, mikäli se tulee näkymään Internetiin. [5]

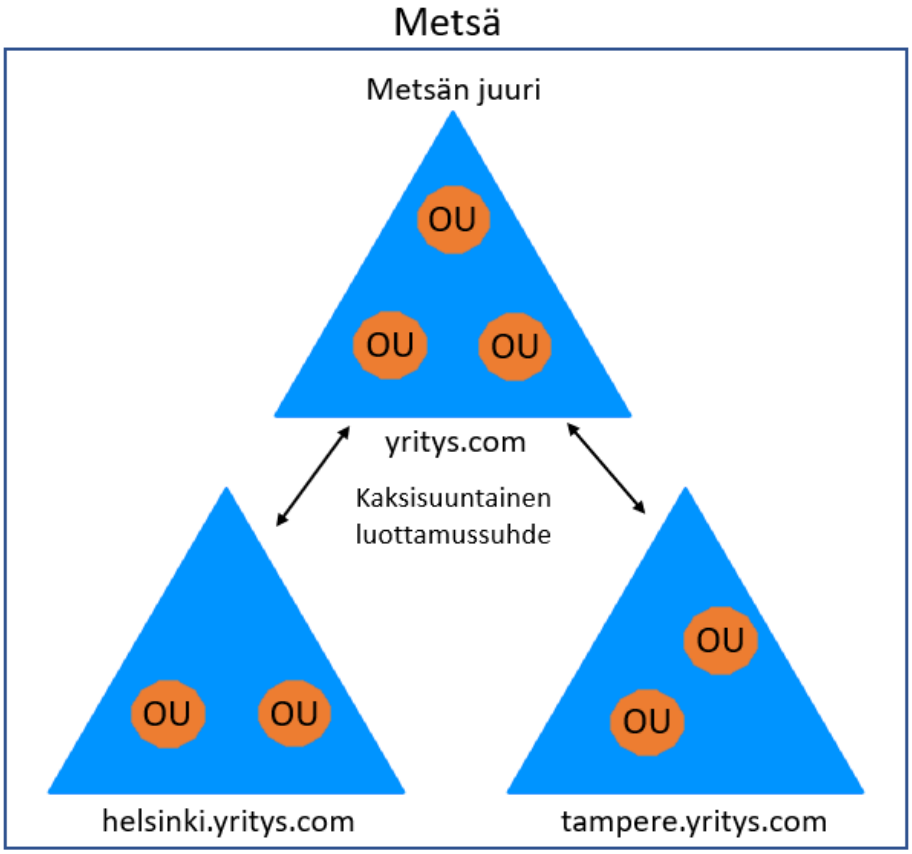
Toimialuepuu

Toimialuepuu tarkoittaa hierarkkisesti muodostettua verkkotunnuspuuta, joka käyttää samaa DNS-nimiavaruutta. Siinä juuritoimialueen alla voi olla alitoimialueita haluttu määrä, esimerkiksi: **yritys.com** toimialueen alle voidaan luoda alitoimialueet **tampere.yritys.com** ja **helsinki.yritys.com**. Nämä toimialueet ovat

osa samaa verkkoaluepuuta ja siinä emo- ja alatason verkkotunnuksien välille luodaan automaattisesti luottamussuhde.

Toimialuemetsä

Toimialuemetsä muodostuu yhdestä tai useammasta toimialuepuusta. Kuvassa 1 on kuvattu toimialuemetsässä ainoastaan yksi toimialuepuu. Toimialuepuut on yhdistetty toisiinsa transitiivisen luottamuksen kautta. Toimialuemetsä luodaan automaattisesti ensimmäisen toimialueen eli Active Directoryn käyttöönoton yhteydessä. Kaikki metsän sisällä olevat toimialueet jakavat niille yhteisen kaavan eli Scheman.



Kuva 1. Metsä, jossa toimialueet kuvattuna

Global Catalog (yleinen hakupalvelu)

Global Catalog (GC) eli yleinen hakupalvelu on Active Directoryn ohjauskoneiden valinnainen ominaisuus, jonka toimesta tarjotaan tietoja koko metsän objekteista. Global Catalog luodaan automaattisesti ensimmäiseen toimialueen ohjauskoneeseen asennuksen yhteydessä. Global Catalog tallentaa kopiot kaikista AD:n objekteista toimialuepalvelimen metsässä ja osittaiset kopiot toisten toimialuepalvelimien eli ns. alidomainien objekteista. GC:n luontainen sijoittelupaikka lienee ainakin metsän laajuisten roolien kanssa samassa ohjainkoneessa.

Global Catalog voi olla käytössä mahdollisesti metsän muissakin ohjauskoneissa tilanteen mukaan, mikäli toimialueen ohjauskoneet esimerkiksi sijaitsevat maantieteellisesti tai verkkotopologisesti kaukana toisistaan. Tällöin mm. käyttäjien kyselyt ja muut hakutoiminnot nopeutuvat ja kirjautumiset järjestelmään nopeutuvat, mikäli Global Catalog sijaitsee lähimpänä olevassa ohjauskoneessa. [4, s.27]

3.1.2 Flexible Single Master Operation (FSMO)

Aktiivihakemiston tietokanta on tallennettuna hajautetusti ohjainkoneille (Domain Controller) ja kaikki ohjainkoneet voivat periaatteessa vastata asiakaskoneiden pyyntöihin. Tietyt kriittisemmät toiminnot on kuitenkin varmuuden vuoksi roolitettava eri ohjainkoneisiin, jotta esim. yhtäaikaiset pyynnöt eivät aiheuttaisi ristiriitoja palvelupyynnöissä. Näiden FSMO-palveluroolien sijoittelu useamman ohjainkoneen ympäristössä on syytä suunnitella huolellisesti. Ohjainkoneiden käytettävyys ja kuormituksen tasaaminen ovat tärkeimpiä huomioitavia seikkoja FSMO-roolituksessa. Yhden ohjainkoneen ympäristössä kaikki FSMO-roolit ovat yhdessä ja samassa ohjainkoneessa. Kun toimialueelle otetaan käyttöön useampia ohjainkoneita käyttöön, tulisi näihin roolien sijaintiin ohjainkoneissa ottaa kantaa. Näitä AD:n tärkeitä toiminnallisia FSMO-rooleja on **viisi kappaletta:** [6]

- Schema master
- Domain naming master
- RID (Relative Identifier) master

- PDC (Primary Domain Controller) emulator
- Infrastructure master.

Näitä FSMO-rooleja voi siirtää tarpeen ja tilanteen mukaan ohjainkoneelta toiselle, mikäli tilanne niin vaatii. FSMO-roolien sijoittelu ohjainkoneisiin oikeaoppisesti on erittäin tärkeää, varsinkin organisaatiossa, joissa käyttäjiä ja tietokoneita on tuhansia ja toimipaikkoja useita. Aiheeseen kannattaa syventyä mm. Microsoftin dokumentaation avulla. [4, s.140] [7]

Schema master roolin omaava kone hallitsee muutoksia, jotka liittyvät metsän kaavan eli skeeman muutoksiin. Tämän roolin luontainen sijoittelupaikka lienee metsän juuritoimialueella sijaitsevassa ohjainkoneessa. Muut ohjainkoneet eivät voi tehdä muutoksia Active Directoryn rakenteeseen. Metsässä voi olla vain yksi tämän roolin omaava ohjainkone.

Domain naming master rooli on metsäkohtainen ja vain yksi metsän ohjainkone voi omata tämän roolin. Tämä päärooli on vastuussa mm. toimialueen ohjainkoneisiin ja nimiavaruuteen liittyvistä muutoksista tai lisäyksistä. Luontainen sijoittelupaikka lienee samassa ohjainkoneessa kuin **Schema master**.

RID (Relative Identifier) master rooli on toimialuekohtainen ja jokaisella toimialueella on oltava yksi tämän roolin omaava ohjainkone. Se vastaa RID-poolipyyntöjen käsittelystä ja on vastuussa objektien siirrosta toiseen toimialueeseen. Uniikki RID-tunniste lisätään toimialueen SID (Security Identifier) -tunnisteeseen. Tämä tunniste luodaan kaikille toimialueen ryhmille, tietokoneille ja käyttäjille eli ns. **security principal** -objekteille. Nämä ovat yksilöllisiä tunnisteita, joiden perusteella jaetaan oikeuksia toimialueen resursseihin. Oletusarvoisesti ohjainkoneille on varattu 500 RID-tunnistetietuetta ja tarvittaessa niitä pyydetään lisää RID-masterilta.

PDC (Primary Domain Controller) emulaattori rooli on toimialuekohtainen ja jokaisella toimialueella pitää olla yksi tämän roolin omaava ohjainkone. Tämän roolin omaavan ohjainkoneen kello tulee synkronoida jostain luotettavasta ulkoisesta aikalähteestä, koska se vastaa toimialueen ohjainkoneiden kellojen

synkronointihierarkiasta. PDC-emulaattori toimii pääselaimena tietokoneille ja hoitaa mm. verkkotunnusten salasanojen replikoinnin muihin ohjauskoneisiin sekä ryhmäkäytäntöjen muutoksien hallinnan. PDC-emulaattori hoitaa myös tilien lukituksen. Tätä roolia ei suositella asennettavaksi samaan ohjainkoneeseen *Infrastructure master* roolin kanssa. PDC-roolin omaava ohjainkone tulee olla saatavilla jatkuvasti toimialueella. Tämä rooli vaatii ohjainkoneelta yleensä eniten tehoja, joten sen sijoittaminen monitoimialueympäristössä mahdollisemman tehokkaaseen ohjainkoneeseen on suositeltavaa.

Infrastructure master rooli on toimialuekohtainen ja sen tehtäviin kuuluu ylläpitää viittauksia objekteihin ja niiden muutoksiin omassa toimialueessa sekä viittauksista objekteihin toisissa toimialueissa. *Global Catalog* -palvelua ei suositella sijoitettavaksi samaan ohjainkoneeseen kuin Infrastructure master roolia. Tätä palvelua eli roolia käytetään melko harvoin ja yhden toimialueen ympäristössä ei juuri lainkaan.

3.1.3 Active Directoryn tietokanta (NTDS.dit)

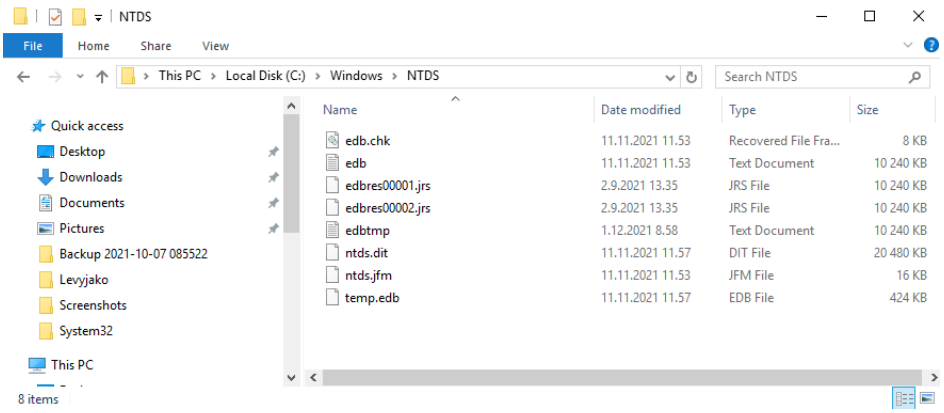
Active Directoryn tietokanta käyttää Microsoftin Extensible Storage Engine (ESE) -tietokantamoottoria. Se on tehokas ja kevyt tiedonhallintatekniikka, joka tunnetaan myös nimellä JET Blue (Joint Engine Technology). Se perustuu Indexed and Sequential Access Method (ISAM) tiedontallennustekniikkaan. Microsoft käyttää sitä myös monissa muissa sovelluksissaan, kuten esim. Microsoft Exchange Server -sähköpostijärjestelmässään. [4, s. 361] [8]

Active Directoryn tietokanta on tallennettu Ntds.dit-tiedostoon (NT Directory Services) ja sijaitsee ohjainkoneen (Domain Controllerin) systeemilevyllä C:\Windows\NTDS-kansiossa. NTDS.dit-tiedosto pitää sisällään kaikki AD:n objektit ja käyttöoikeudet. Tietokanta on salatussa muodossa, koska sisältönä on mm. kaikkien käyttäjien salasanojen tiivisteet (”hashit”). Tietokannan sisäinen rakenne jakaantuu loogisesti neljään eri osioon, jotka ovat:

- kaavaosio (schema partition)

- konfiguraatio-osio (configuration partition)
- toimialueosio (domain partition)
- sovellusosio (application partition).

NTDS.dit-tiedoston sisältö replikoituu toimialueen mahdollisiin muihin ohjainkoneisiin niiltä osin, mikä on tarpeellista toiminnan kannalta. Samassa kansiossa systeemilevyllä on NTDS.dit-tiedoston lisäksi joitakin muita tärkeitä tietokannan toimintaan ja hakemistotapahtumiin liittyviä aputiedostoja (kuva 2).



Kuva 2. NTDS-kansion sisältö

- Ntds.dit, sisältää kaikki AD:n objektit ja jakaantuu loogisesti neljään osioon: Schema Partition, Configuration Partition, Domain Partition, Application Partition.
- Edb.log, tietokannan tapahtumaloki (transaction log).
- Edb.chk, tietokannan tarkistustiedosto (checkpoint-tiedosto).
- Res1.log ja res2.log (edbres0001.jrs ja edbres0002.jrs), tilanvaraus lokitiedoille levytilan loppuessa.
- Temp.edb, hakemistotapahtuman aputiedosto.

3.2 Palvelininfrastruktuurin suunnittelu

Palvelininfrastruktuurin ja Active Directoryn suunnittelu tulee tehdä aina huolellisesti. Organisaatioita on eri kokoisia ja suurien kansainvälisten organisaatioiden palvelininfrastruktuurin tai hakemistopalvelun suunnittelu vaatii luonnollisesti laajaa ja tarkkaa yhteistyötä eri toimijoiden kesken. Organisaation

kokonaisvaltaisessa Active Directoryn suunnittelussa on huomioitava verkkoon liittyvät rakenteet, kuten DNS-nimiavaruus ja verkkoyhteydet mahdollisiin eri toimipisteiden toimialueisiin. Verkkoyhteyksien on toimittava luotettavasti ja sujuvasti eri toimialueiden kesken ja luottosuhteet niiden välillä tulee olla kunnossa. [4, s. 116, 156]

Tietoturvallisuuteen tulee kiinnittää erityistä huomiota, koska Active Directory on ylivoimaisesti kaikkein kriittisin järjestelmä organisaation ICT-infrastruktuurissa. Toisaalta nykyisin esim. Microsoftin Azure -pilvipalvelut tarjoavat kuitenkin paljon mahdollisuuksia erilaisiin virtuaalisointiratkaisuihin, jolloin ihan kaikkea ei tarvitse rakentaa itse. Yleensä suositellaan ennen varsinaista AD-migraatiota, että rakennetaan erillinen *virtuaalinen testiympäristö*, jossa voidaan testata miten AD-migraatiossa tehtävät muutokset todennäköisesti tulevat vaikuttamaan tuotantoympäristöön.

Tässä työssä oli kysymys tietokoneluokan paikallisesta opetusympäristön kehitysprojektista. Lisäksi tietokoneluokkaympäristö ei ole kovin kriittinen ja migraatiossa huomioidaan mm. palvelimen vikaantuminen siten, että paikallisten tunnuksien käyttö on aina mahdollista työasemilla. Verkkoyhteydet toimivat ilman AD-palvelintakin tai ainakin ne saadaan toimimaan melko helposti, mikäli palvelin lakkaa toimimasta. Erillistä virtuaalista testiympäristöä ei tässä tapauksessa koettu tarpeelliseksi rakentaa.

ICT-tuotannossa maailmalla ollaan yleisesti menossa kovaa vauhtia *virtualisoituihin ympäristöihin ja pilvipalveluihin*, joten niitä kannattaa harkita rakennettaessa oman organisaation ICT-ympäristöä. Usein ns. hybridiratkaisut ovat suosittuja, jolloin osa ICT-tuotannosta hoidetaan itse ja osa ulkoistetaan. Seuraavassa osiossa kerrotaan joitakin seikkoja liittyen virtualisointiin ja pilvipalveluihin yleisesti.

3.3 Virtualisointi ja pilvipalvelut

Verkkotekniikoiden ja verkkojen kehittyessä parin viime vuosikymmenen aikana riittävän nopeiksi ja luotettaviksi, alettiin tarjoamaan organisaatioille yleisesti ns. pilvilaskentaa (cloud computing) eli pilvipalveluita (cloud service). Tämä tarjoaa yrityksille kätevän ja joustavan mahdollisuuden hankkia tietotekniikkapalveluita ikään kuin tuotteena niitä tarjoavilta asiantuntijayrityksiltä. Pilvilaskentaa tarjoavat asiantuntijayritykset ovat usein maailmanlaajuisia ja isoja toimijoita, kuten Microsoft Azure, Amazon Web Services (AWS), IBM, Salesforce, Google.Cloud ja SAP. [9]

Virtualisointi

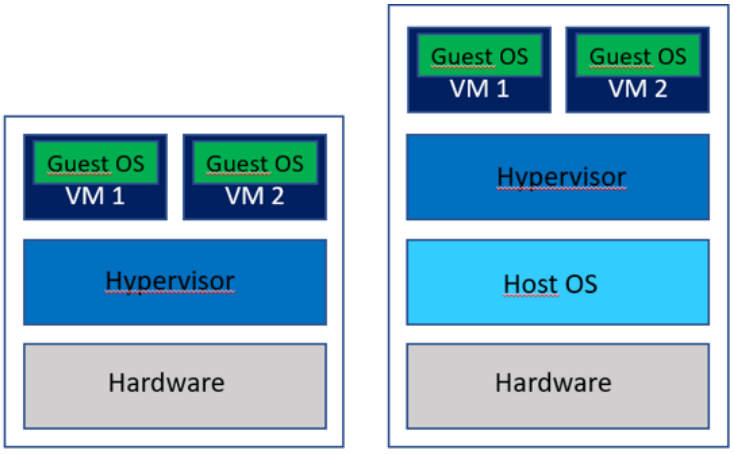
Tietotekniikassa virtualisointi tarkoittaa tietoteknisen resurssin esitystä abstraktilla tasolla. Virtuaalinen laite piilottaa todellisen fyysisen laitteen loogisia resursseja käyttäviltä olioilta. Monia tietoteknisiä resursseja voidaan virtualisoida kuten: palvelimia, muisteja, verkkoja, verkkolaitteita, tallennustiloja, työasemia ja sovelluksia. Eniten käytetty virtualisoinnin osa-alueista lienee laitevirtualisointi eli palvelinvirtualisointi. Siinä palvelinlaitteistoa hyödynnetään useampana laitteena eli virtuaalipalvelimena. Toisin sanoen palvelinlaitteiston resurssit muutetaan loogisiksi resursseiksi, joita sitten virtuaalipalvelimet voivat käyttää. [10]

Palvelinvirtualisoinnin avulla voidaan parantaa dramaattisesti laitekannan käytön hyötysuhdetta eli käytettävyysastetta. Resursseja voidaan allokoida joustavasti sinne, missä niitä tarvitaan. Virtuaalipalvelimien asennus ja käyttöönotto on nopeaa ja kohtuullisen helppoa. Tietoturva, etenkin vikasietoisuus sekä tiedonsiirto- ja tallennustekniikat ovat korkealla tasolla. Virtuaaliympäristön hallinta on sujuvaa ja varmuuskopioiden, tilanne- ja levykuvien ottaminen on helppoa sekä nopeaa. Hallintasovelluksilla voi myös kätevästi automatisoida erilaisia haluttuja toimintoja. Tämän lisäksi virtualisointi säästää kustannuksia ja on energiatehokasta sekä lähtökohtaisesti ympäristöystävällistä tekniikkaa.

Palvelinvirtualisointiin tarvitaan erillinen ohjelmisto eli virtuaalikonemonitori (Virtual Machine Monitor, VMM) eli nykyisin *Hypervisor*. Se on isäntäjärjestelmään

asennettu virtualisointikerros, joka mahdollistaa useiden virtuaalikoneiden ajamisen pääjärjestelmässä. Hypervisorit voidaan jakaa kahteen eri päätyyppiin: laitteiston päällä ikään kuin natiivisti suoritettava täysvirtualisointi **Tyyppi 1** ja isäntäkäyttöjärjestelmän alaisuudessa (Host OS) suoritettava käyttöjärjestelmätason virtualisointi **Tyyppi 2**. Kuvassa 3 on esitetty virtualisointityypit 1 ja 2.

Hypervisorien päällä toimivia virtuaalikoneita (Virtual Machine, VM) kutsutaan vieraskäyttöjärjestelmiksi (Guest OS). Vieraskäyttöjärjestelmät havaitsevat vain niille emuloidut resurssit, eivätkä ne ole tietoisia isäntäkoneen resursseista. Eri virtuaalikoneet (esim. VM1 ja VM2) ovat eristyksissä toisistaan ja yhden virtuaalikoneen mahdolliset ongelmat ja häiriöt eivät vaikuta toiseen. Toisaalta isäntäkoneen ongelmat ja häiriöt vaikuttavat pahimmillaan kaikkiin virtuaalikoneisiin. Tästä johtuen isäntäkoneen laitteisto ja käyttöjärjestelmä pyritään saamaan mahdollisimman vakaaksi ja vikasietoiseksi.



Kuva 3. Virtualisointityypit

Pilvipalvelut (pilvilaskenta)

Pilvipalvelut eli ts. pilvilaskenta tarkoittavat erilaisten hajautettujen tietoteknisten palveluiden tarjoamista verkon (internetin) kautta. Nämä palvelut ovat yleensä pitkälle virtualisoitujen järjestelmien päällä toimivia. Pilvipalveluista mainittakoon mm. sovellukset, työkalusovellukset, ohjelmistot, tietojen tallennus, palvelimet, tietokannat ja verkot. Palvelimet, järjestelmät ja tietokannat sijaitsevat siis verkossa jossain palveluntarjoajan palvelimella tai palvelinkeskuksissa jossain päin maailmaa. Palvelut ovat saatavilla aina kun yhteys verkon kautta on mahdollista ja käytettävissä on päätelaite. Tämän kaltainen toimintamalli asettaa verkolle korkeat Service-Level Agreement (SLA) -vaatimukset.

Pilvi, josta pilvipalvelut tarjotaan voi olla tyypiltään julkinen, yksityinen tai niiden yhdistelmä. Pilvipalveluita (julkisia) tarjoavat suurehkot toimijat kotimaassa ja ulkomailla. Datakeskukset sijaitsevat yleensä kattavasti ympäri maailman ja asiakkaan sijainnista riippuen palvelut tarjotaan lähimmästä datakeskuksesta. Pilvipalvelut ovat erittäin suosittu ja joustava tapa hankkia ICT-tuotantopalveluita. Tärkeimmät syyt pilvipalveluiden valintaan lienevät: korkea käytettävyysaste, kustannussäästöt (laitteet, tilat ja henkilöstö), saavutettavuus, joustavuus, skaalautuvuus, tehokkuus, tuottavuus, nopeus, suorituskyky, energiatehokkuus, tietoturvallisuus, valvontaominaisuudet ja ympäristöarvot.

Tietoturvataso pilvipalveluissa on yleensä kohtalaisen hyvä, koska pilvipalveluita tarjoavat yritykset ovat raskaan sarjan ammattilaisia, kuten Microsoft Azure, Google ja Amazon Web Services (AWS). On kuitenkin todettava, että tietoturvaongelmat eivät katoa mihinkään ottamalla käyttöön pilvipalveluita, vaan ne muuttavat muotoaan toisenlaisiksi. Pilvipalveluissa on monia eri käyttö- ja hallintarajapintoja ympäriinsä ja niiden tietoturvataso voi vaihdella, joten tutustuminen palveluntarjoajan tietoturvakonseptiin on hyvinkin suotavaa. Pilvipalveluissa on omanlaisensa tietoturvaongelmat ja ei ne kyberrikolliset mihinkään katoa.

Perustavaa laatua oleva ongelma on se, missä tiedot sijaitsevat ja minkä valtion säädöksien alla niitä säilötään. Eri pilvipalvelutyypeillä on myös eriävät

tietoturvaongelmat ja niiden itsenäinen hallinta ei aina ole mahdollista, vaan lähes kaikki voi olla palveluntarjoajan käsissä. Asianmukaisten ja selkeiden sopimuksien tekeminen palveluntarjoajan kanssa on kuitenkin hyvä lähtökohta. Yrityksien ei kannata kuitenkaan välttämättä ulkoistaa kaikista tärkeimpiä ja toiminnalleen arvokkaimpia asioita eli ns. ”kruunun jalokiviä”, vaan ne on syytä pitää omissa käsissään ja huomassaan.

Pilvipalveluiden hallinta on yleensä kohtuullisen vaivatonta, vaikkakin uuden kulttuurin omaksumiseen menee hiukan aikaa. Pilvipalveluiden hallintatapoja webportaalin lisäksi on monia ja niistä kerrotaan lisää kohdassa **5.3. Pilvipalvelujen etähallintaratkaisut**. Hyvä asia on myös se, että usein pilvipalvelujen palvelupakettiin kuuluu runsaasti myös ilmaisia palveluja, jotka parantavat palvelupaketin laatua. Pilvipalveluista maksat vain siitä mitä käytät ja järjestelmät skaalautuvat tarpeen mukaan, jopa automaattisesti. Nykyisin lähes jokainen organisaatio käyttää jotakin pilvipalvelutyyppiä. Kuvassa 4 on esitetty yleisimmät pilvipalvelumallit. (Kuva: Microsoft Windows Azure)

Pilvipalvelutyypit

Tärkeimmät pilvipalvelutyypit ovat:

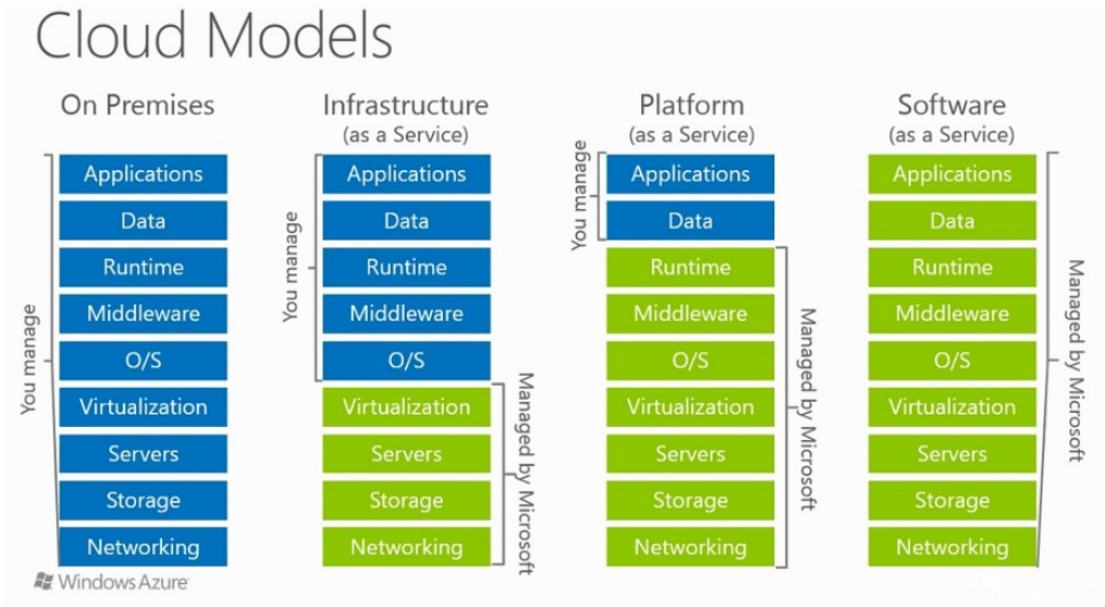
- Infrastruktuuri palveluna (Infrastructure as a Service, IaaS).
- Alusta palveluna (Platform as a Service, PaaS).
- Ohjelmisto palveluna (Software as a Service, SaaS).

Nykyisin on tarjolla myös muita ratkaisuja kuten:

- Säiliö palveluna (Container as a Service, CaaS).
- Toiminnot palveluna (Function as a Service, FaaS).
- Työpöytä palveluna (Desktop as a Service, DaaS).

Yhteisesti voidaan nimittää kaikkia pilvipalveluita Anything as a Service (XaaS) -palveluiksi ja X voidaan muuttaa halutuksi palveluksi. Keskitymme kolmeen

tärkeimpään pilvipalvelutyyppiin (IaaS, PaaS ja SaaS). Kuvassa 4 esitetään tärkeimmät pilvipalvelumallit. [11]



Kuva 4. Tärkeimmät pilvipalvelumallit [Microsoft Windows Azure]

Infrastruktuuri palveluna (IaaS)

Hankittaessa infrastruktuuripalveluita (Infrastructure as a Service) pilvestä on siinä kysymys usein virtuaalikoneiden hankkimisesta. Ylläpitäjä vastaa siinä itse virtuaalikoneiden määrittämisestä, käyttöjärjestelmästä, verkkoasetuksista, ohjelmistoista ja tiedoista. Tämä malli auttaa vähentämään kustannuksia paikallisten palvelinkeskusten laitekustannuksissa ja niiden ylläpidossa. Palvelinsalia ei tällöin tarvita ja siihen liittyvät kustannukset vähenevät tai niitä ei ole lainkaan. Infrastruktuuripalvelut ovat myös nopeita ottaa käyttöön ja IT-resurssit ovat skaalattavissa tarpeen mukaan joustavasti, jopa automaattisesti kysynnän mukaan. Mallissa maksat vain siitä, mitä käytät, jolloin hyötysuhde ja käytettävyysaste on hyvä.

Alusta palveluna (PaaS)

Alustan hankinta (Platform as a Service) palveluna tarkoittaa yleensä sovellusalustaa, jonka palveluntarjoaja tarjoaa ja vastaat siinä itse vain tarjottavasta sovelluksesta ja sen määrittelystä sekä sen sisäisestä tietoturvasta. Tämä PaaS-ratkaisu on kevyempi hallita kuin IaaS ja soveltuu hyvin esim. ohjelmistokehitysprojekteihin, tietokannan pyörittämiseen tai WWW-palveluihin (kuva 4).

Ohjelmisto palveluna (SaaS)

Ohjelmistoa palveluna (Software as a Service) on kevein ja yksinkertaisin ratkaisu. Palveluntarjoaja tarjoaa siinä tarvittavat ohjelmistot käyttäjälle ajantasaisena webin kautta. Käyttäjän vastuulle jää vain ohjelmistojen käyttö ja jakelu. Tämä lienee helppohoitoisin ja suosituin pilvipalvelutyyppi perussovelluksien tarjontaan, esim. Microsoftin Office 365 ja sähköpostipalvelut (kuva 4).

3.4 Azure Active Directory (AAD)

Microsoftin Azure Active Directorya käytetään todennukseen ja valtuutukseen pilvipalveluissa. Microsoftin tarjoamat Online-palvelut, kuten Microsoft Office 365, sisältää automaattisesti Azure AD:n palvelut taustalla. Azure AD tarjoaa kirjautumispalveluita, identiteetin ja lisenssien hallintaa Microsoftin Online-palveluihin. Azure AD tarjoaa organisaatiolle tavallaan *Identity as a Service (IDaaS)* -ratkaisun kaikille sovelluksilleen pilvessä. Halutessaan organisaatio voi liittää eli synkronoida Azure AD:n omaan paikalliseen Active Directoryyn. [4, s. 41]

Azure Active Directory eroaa selkeästi varsinaisesta perinteisestä hakemistopalvelusta (Active Directory Domain Services, AD DS), eikä se korvaa sitä sellaisenaan. Azure AD:ssä ei ole samanlaisia ryhmäkäytäntöjä (Group Policy) käytettävissä kuin AD DS -ratkaisussa, eikä samanlaista organisaatioyksikköihin perustuvaa rakennetta kuin perinteisessä Active Directoryssa. Se tarjoaa kuitenkin organisaatiolle monia joustavia mahdollisuuksia ICT-tuotantopalve-

luiden järjestämiseen. Mikäli organisaatiolla on kaikki ICT-palvelut Microsoftin pilvessä, niin Azure AD on siihen luonnollisesti paras ratkaisu.

Azuren AD:n sovellushallinta käyttää nykyaikaisia todennusmekanismeja, kuten Security Assertion Markup Language (SAML) ja OAuth. Perinteisessä AD DS:ssä olevat liikennöintiprotokollat ovat vastaavasti LDAP ja Kerberos. Azure AD tarjoaa saumattoman yhteyden tuhansiin SaaS-sovelluksiin pilvipalveluissa ja vieläpä kertakirjautumisella (Single Sign-On, SSO). Valmiita integraatioita SSO-ratkaisulle löytyy tuhansia Azure AD:ssa. Tämän lisäksi Azure AD:hen on integroitavissa (mobiili)laitteiden hallintaratkaisu nimeltään Microsoft Intune. Hallintamahdollisuudet tietokoneille ovat kuitenkin rajatumpia verrattuna perinteiseen Active Directoryyn. Tietoturva ja käyttäjille tarjottavat todennusmenetelmät ovat Azure AD:ssa korkealla tasolla ja statistiikkaa saa kätevästi kerättyä sovelluksista ja niiden käytöstä.

Perinteinen Active Directory lienee paras vaihtoehto paikallisen infrastruktuurin monipuoliseen hallitsemiseen. Monilla organisaatiolla on usein käytössä ns. yhdistelmä- eli hybridiratkaisuja. Yritys voi esim. hankkia Office 365 palvelut pilvestä ja hallita paikallista laiteinfraansa ja käyttäjätunnuksiaan perinteisellä hakemistopalvelulla. Käyttäjätunnukset paikallisesta AD:stä voidaan helposti synkronoida pilvipalveluun, jolloin käyttäjien ei tarvitse kirjautua erikseen esim. Office 365 -palveluihin.

Hybrid Active Directory

Oman paikallisen hakemistopalvelun (AD DS) voi synkronoida Azure AD:hen ja alkuun pääsee maksuttomalla Azure AD -lisenssilläkin, mikäli esim. Office 365 palvelut ovat käytössä entuudestaan. Microsoftilla on tarjolla myös enemmän ominaisuuksia sisältävät maksulliset AAD:n Premium P1 ja P2-lisenssit. Synkronointi järjestelmien välillä voidaan tehdä **Azure AD Connect** -työkalulla, jolloin käyttäjien todennus paikallisiin resursseihin ja pilvessä toimiviin sovelluksiin toimii tarvittaessa kertakirjautumisella (SSO). Azure AD Connect -työkalusta on julkaistu kirjoitushetkellä versio 2. [4, s.618] [12]

Azure AD DS

Microsoftilla on myös tarjolla pilvessä pyöritettävä AD DS -palvelu. Se tarjoaa pilveen siirrettäville vanhoille ja perinteisiä liikennöintiprotokollia (LDAP, Kerberos/NTLM (New Technology Lan Manager)) käyttäville sovelluksille järjestelmäratkaisun. Ratkaisu ei vaadi erillistä ohjainkonetta, eikä asiakkaan tarvitse ottaa kantaa ohjainkoneiden ylläpitoon pilvessä. Voidaan yhdistää myös paikalliseen Active Directoryyn.

3.5 Palvelinalustan valinta

Valitessaan alustaa palvelinohjelmistoille, tulee huomioida muutamia tärkeitä asioita, kuten monet tietoturvaan liittyvät asiat, käytössä olevat henkilöstöresurssit, tilat, verkot, kustannukset, järjestelmän skaalautuvuus, joustavuus, lainsäädäntö ja enenemässä määrin myös kestävään kehitykseen liittyvät seikat kuten energiatehokkuus ja ympäristöarvot.

Tänä päivänä tarjotaan monia pilvipalveluratkaisuja, joita organisaation kannattaa harkita ainakin osaan tarjottavista ICT-palveluistaan. Kaiken voi periaatteessa ulkoistaa ja jokaisessa ratkaisuissa on omat hyvät ja huonot puolensa. Monesti hybridiratkaisut ovat käyttökelpoisia ja usein järkevin sekä suositeltavin valinta organisaation ICT-tuotantomalliin. Organisaation tulee riskiarvioinnin avulla kartoittaa oman toimintasektorin riskit ja vaadittavat tietoturvallisuustasot. Tarvitseeko palvelimien kestää luonnonkatastrofit ja mahdolliset asevaikutukset vai riittääkö tavanomaiset perustason suojaukset. Tässäkin laatu ratkaisee ja kannattaa käyttää asiantuntijoita apuna ja investoida myös henkilökunnan koulutukseen, se maksaa kyllä itsensä takaisin.

Perinteinen rautapalvelin

Tässä työssä laitealustaksi valittiin perinteinen rautapalvelin, joka löytyi entuudestaan mikrotuen siirtovarastosta. Palvelin oli ollut useamman vuoden primäärikäytössä ja oli siirtymässä toisiokäyttöön. Tarkoitus oli hyödyntää vanha

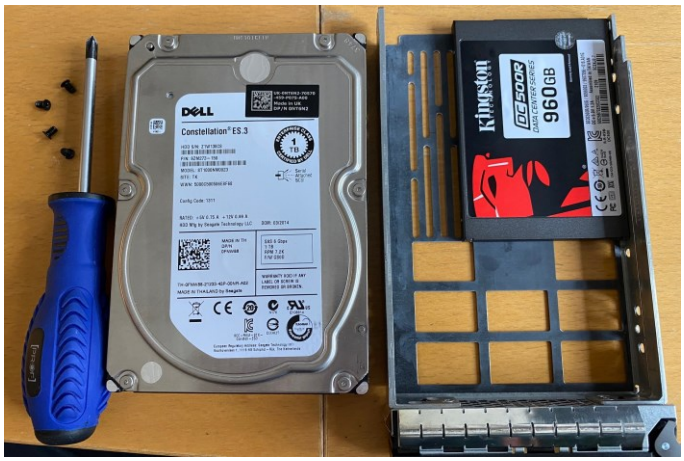
palvelinrauta niiltä osin kuin osat ovat soveltuvia ja riittäviä käyttötarkoitukseen. Palvelinta tarkisteltaessa todettiin, että ainakin kovalevyjen osalta tarvitaan päivitys. Lisäksi asennusvaiheessa palvelin tarkistettiin ulkoisesti ja puhdistettiin pölyt laitteiston sisältä pois.

Palvelin, johon Microsoftin Windows Server 2016 Standard Edition käyttöjärjestelmä asennettiin, on Dellin PowerEdge T320 Server. Se on muutaman vuoden vanha perinteinen tornimallinen palvelin (kuvassa 5). Palvelimen teknisiä tietoja laitepäivityksen jälkeen: [13]

- prosessorit: Intel Xeon CPU E5-2403 v2, 1,8 Ghz (Neljä ydintä)
- RAM: 32 GB
- SSD: 2 x 960 GB
- levyohjain: Dell PERC H310 SCSI (PCI Express 2.0)
- 2 kpl 960 GB SSD-levyä (SATA III 6 Gbps, lukunopeus 555 Mt/s), Hot Plug
- virtalähde kahdennettu: Hot Plug, reduntant 495 W
- 2 kpl verkkoliitäntää: Broadcom 5720 Dual Port 1 Gbit LOM
- GPU: NVIDIA Quadro 4000
- muut liitännät: USB2, VGA
- etähallinta: iDRAC7 (Integrated Dell Remote Access Controller 7).

Kuva 5. Dell PowerEdge T320 tornipalvelin

Vanhaa rautapalvelinta päivitettiin, siten, että siihen vaihdettiin kaksi SSD-levyä perinteisten pyörivien kovalevyjen (SAS 6 Gbps, 1 TB, RPM 7.2K) tilalle (kuva 6). Asennettavat SSD-levyt (SATA III 6 Gbps, lukunopeus 555 Mt/s) valittiin siten, että ne ovat optimoituja lukupainotteiseen palvelinkäyttöön. SSD-levyjen koko on 960 Gtavua ja niitä tarvittiin kaksi kappaletta, koska tarkoituksena oli ottaa käyttöön vikasietoinen ja laitteistopohjainen RAID 1 -levyjärjestelmä.



Kuva 6. Perinteinen kovalevy ja uusi SSD-levy

3.6 Palvelimen käyttöönotto (hardware)

Palvelinraudan käsittelyssä tulee olla huolellinen, koska staattinen sähkö voi rikkoa herkkiä puolijohteita tai lyhentää komponenttien elinikää. Kriittisissä kokoonpanotöissä tulee käyttää mm. maadoitusranneketta ja siihen tarkoitettua alustaa. Tässä palvelimen asennustyössä käytettiin lisäksi pääsääntöisenä työkaluna ristipääruuvitalttaa. Perinteiset kiintolevyt vaihdettiin SSD-levyihin, jotka ovat optimoituja palvelinkäyttöön. SSD-levyjen kiinnittämisessä jouduttiin hiukan ”säätämään”, jotta saatiin ne levykelkkoihin oikeisiin kohtiin kiinnitettyä, kuten kuvassa 6 yläpuolella näkyy.

Kokoonpanon jälkeen kytkettiin näyttö palvelimen VGA-liitäntään ja näppäimistö sekä hiiri USB-liitäntään. Lopuksi kytkettiin virtajohdot palvelimen virtalähteisiin ja näyttöön. Testikäynnistyksen jälkeen tutustuttiin *BIOS-asetuksiin ja RAID-ohjaimen määrittelyyn*.

Palvelimen käynnistyksen yhteydessä pääsee erilaisiin alkuasetuksien määrittelyihin painamalla jotakin tiettyä näppäintä tai niiden yhdistelmää. Dellin palvelimessa olevia tärkeitä ns. ”taikanäppäimiä” ovat mm.

- F2 System Setup
- F10 Lifecycle Controller
- CTRL-S Verkkokortin määrittely
- CTRL-R RAID Controller BIOS.

Määriteltiin BIOS:ssa RAID 1 taso käyttöön ja nimettiin virtuaalilevy sekä initialisoitiin SSD-levyt (kohdassa 5.2 sivulla 64 kerrotaan tarkemmin RAID-järjestelmistä).

3.7 Toimialuepalvelin (ohjainkone, Domain Controller)

Toimialuepalvelimen (ohjainkoneen) eli Active Directoryn käyttöönottoon tarvitaan Microsoftin Windows Server -ohjelmistolisenssi ja laitealusta mihin palvelinkäyttöjärjestelmä asennetaan. Tämän lisäksi tarvitaan kaikille käyttäjille tai laitteille ns. CAL-lisenssit (Client Access License). Käyttöjärjestelmälisenssien vaihtoehdot ovat yleisesti: Windows Server Standard Edition, Windows Server Datacenter Edition tai Windows Server Essentials-versio pienyrityksille (max. 20 käyttäjää ja 50 laitetta). [14]

Tässä työssä käytimme saatavilla olevaa *Windows Server 2016 Standard Edition -lisenssiä* ja olemassa olevia konekohtaisia CAL-lisenssejä. Tarkoitus on myöhemmin päivittää palvelimen käyttöjärjestelmä uudempaan Windows Server 2019 SE -versioon, mikäli nyt asennettava ratkaisu osoittautuu toimivaksi. Yleisesti lisenssien hinnoittelut löytyvät Microsoftin sivuilta. Windows Server Datacenter Edition lisenssin hinta on moninkertainen ja se on tarkoitettu pitkälle virtualisoituihin datakeskuksiin ja isoihin pilviympäristöihin.

Tässä työssä otettiin aluksi käyttöön vain yksi fyysinen *ohjainkone eli Domain Controller (DC)*. Yhdellä ohjainkoneella pärjätään toistaiseksi, koska käyttöympäristönä on vain paikallinen tietokoneluokka, eikä se ole kovinkaan kriittinen.

Yleensä Active Directoryyn on syytä liittää vähintään kaksi ohjainkonetta vikasietoisuuden kasvattamiseksi.

Asennettiin Windows Server 2016 Standard -versio USB-asennustikulta ja määriteltiin tarvittavat alkuasetukset. Tutkittiin laitteistopuolen ajurien ajantasaisuus ja päivitettiin tarvittaessa. Aktivoitiin Windows-käyttöjärjestelmä ja päivitettiin se ajan tasalle Windows Updaten kautta. Lopuksi skannattiin käyttöjärjestelmä varmuuden vuoksi ajantasaisella Defender-antivirusohjelmalla.

3.8 Active Directoryn käyttöönotto (AD DS)

Alustan valmistelu

Palvelimen asennuksessa tulee huomioida muutama seikka ennen varsinaisen Active Directory Domain Services (AD DS) -roolin käyttöönottoa. Palvelimen nimeämiseen on hyvä käyttää muutama hetki, jotta koneelle saadaan kuvaava ja looginen nimi. Verkkoasetukset tulee olla kunnossa. Palvelimelle on määritettävä staattinen verkko-osoite eli IP-osoite (Internet Protocol), joka on kyseisessä aliverkossa vapaana ja varattuna palvelinkäyttöön.

Palvelimelle tulee määritellä *staattisen IP*-osoitteen lisäksi tarvittavat muut verkkoasetukset käsin, kuten verkkopeite (netmask) ja oletusyhdyskäytävä (default gateway). DNS (Domain Name System) –palvelun asetukset tulee olla lähiverkon mukaiset ja yhteydet internetiin niin ikään kunnossa. Verkkomääritykset tehdään usein vain IPv4-puolelle, koska hyvin harvoissa verkkoympäristöissä vielä käytetään aktiivisesti IPv6-versiota. Toisaalta palvelimelle voidaan tässä tapauksessa jättää IPv6-tuki päälle, koska uudet sovellukset saattavat käyttää sitä sisäisessä toiminnassaan.

Määritettiin sopiva ja looginen nimi palvelimelle (tulevalle ohjainkoneelle), jonka jälkeen varattiin mikrotuen kautta sopiva staattinen IP-osoite ja konfiguroitiin sopivat verkkoasetukset palvelimeen. Tämän jälkeen palvelin käynnistettiin uudelleen ja verkon toimivuus testattiin.

Domain Name System (DNS) ja Active Directory

Domain Name System (DNS) eli nimipalvelujärjestelmä muuntaa verkkotunnuksia IP-osoitteiksi ja toisin päin. Internetissä ja kaikissa verkoissa tietokoneet ja laitteet kommunikoivat keskenään numeeristen IP-osoitteiden avulla. Ihmiset eli järjestelmien käyttäjät tarvitsevat kuitenkin selväkieliset nimet vaikeasti muistettaville IP-osoitteille. Tästä syystä tarvitaan nimipalvelua. [15]

Active Directoryn toiminta on hyvin riippuvainen DNS:n luotettavasta toiminnasta. Verkon ja DNS-nimiavaruuden oikeanlainen toimiminen muodostaa pohjan luotettavalle ja nopealle Active Directoryn toiminnalle. Active Directoryn DNS-nimiavaruus voi noudatella yrityksen ulkoista internetiin näkyvää DNS-nimiavaruutta tai se voi olla myös sisäinen, palomuurin takana oleva ja eri niminen. Muodostettaessa sisäistä nimiavaruutta, voidaan käyttää ylimmän tason toimialuetunnuksen verkkopäätettä (**.local)**. Active Directoryn toimialueen nimeksi voisi näin ollen määrittää esim**. Toimialueennimi.local**.

Microsoft suosittelee Active Directoryn käyttöönotossa *AD-integraded DNS -ratkaisumallin* käyttöönottoa. Tämä tarkoittaa sitä, että organisaation DNS-palvelun tulisi pyöriä samalla palvelimella kuin Active Directoryn. Tällöin AD-palvelin tallentaa verkkovyöhykkeet suoraan omaan tietokantaansa, eikä tarvita erillistä DNS-replikointitopologiaa. Erityisesti koko organisaation ratkaisuissa ja useiden ohjainkoneiden kesken replikointi on tällöin suoraviivaisempaa ja nopeampaa. [16]

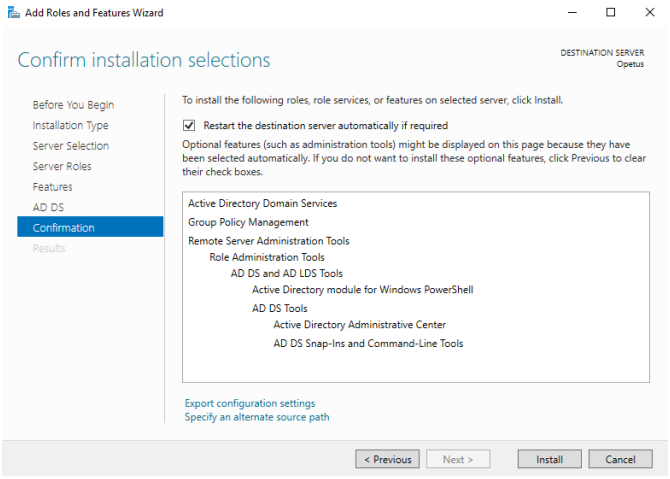
Tässä työssä asennettavan AD-palvelimen (yksi ohjainkone) lähiverkkoympäristön DNS- ja DHCP-palvelut pyörivät erillisellä aktiivilaitteella, eikä niitä lähdetty muuttamaan. Tässä tietokoneluokan paikallisessa ratkaisussa valittiin sisäiseen DNS-nimiavaruuteen perustuva ratkaisumalli ja *AD-integraded DNS -ratkaisu.*

Asennettiin Active Directory (AD DS) Microsoftin suosittelemalla tavalla. Ennen kuin korotimme palvelimen toimialueen ohjauskoneeksi, olimme ennakkoon miettineet sopivaa nimeä toimialueelle. Koko organisaation kattavassa järjestelmäratkaisussa Microsoft suosittelee käytettäväksi yrityksen julkista palvelimen nimeä

eli toimialuetta, esim. **yritys.com**. Tässä työssä käytämme lokaalia toimialueen nimeä (toimialueennimi.local), koska ratkaisu on paikallinen.

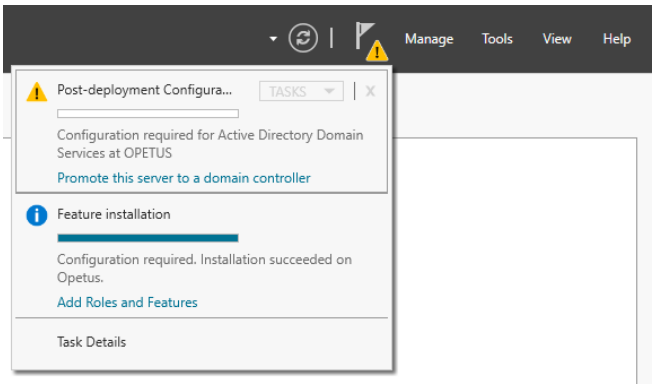
3.8.1 Active Directory Domain Services -roolin asennus

AD DS-roolin lisääminen palvelimeen aloitettiin Server Managerin etusivulta kohdasta: **Add roles and features** **Role-based or feature-based installation**. Kuvassa 7 esitetään kooste asennettavista osista.



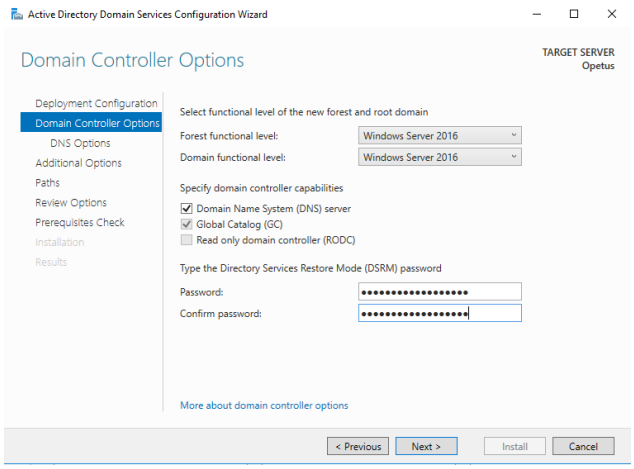
Kuva 7. AD DS asennettavat osat yhteenvetona

Asennuksen jälkeen korotettiin palvelin toimialueen ohjainkoneeksi (Promote this server to a domain controller), kuten kuvasta 8 ilmenee.



Kuva 8. Palvelimen korottaminen toimialueen ohjainkoneeksi (DC)

Asennusohjelma eteni siten, että luotiin ensin uusi metsä (Forest) ja valittiin sopiva ja kuvaava nimi toimialueelle (esim. nimi.local). Valittiin tämän jälkeen korkeimmat mahdolliset toimintatasot metsälle ja toimialueelle (kuva 9). Huomioitavaa toimintatasojen valinnassa on se, mikäli aikaisemmassa palvelinympäristössä olisi vanhemman sukupolven ohjainkoneita, niin ne saattaisivat estää korkeimman toimintatason valinnan. Tässä työssä ja yhden ohjainkoneen ympäristössä valittiin luonnollisesti korkeimmat tarjolla olevat toimintatasot.



Kuva 9. DC:n ominaisuudet ja DSRM-salasana

Tässä yhteydessä luotiin myös hakemistopalvelun palautussalasana eli **Directory Services Restore Mode (DSRM)** tilin salasana palvelimelle. Salasana kannattaa säilöä varmaan talteen. Tätä salasanaa tarvitaan, jos joudutaan joskus palauttamaan palvelin. Tämän jälkeen hyväksyttiin asennusohjelman ehdottama NetBIOS-nimi palvelimelle ja oletusasennuskansioiden sijainnit. Muutama oletettu virheilmoitus tuli asennuksen aikana, mutta ne eivät estäneet asennuksen etenemistä. Uudelleen käynnistyksen jälkeen kirjauduttiin Administrator-tunnuksella toimialueelle. Asennus näytti onnistuneen ja kirjautuminen palvelimelle onnistui.

Huomiona voisi todeta, että asennustöissä käytetään yleensä asennusohjelman tarjoamia oletuskansioita, mutta erityisen kriittisissä järjestelmissä voidaan

järjestelmää ”kovettaa” vaihtamalla oletuskansiorakenne joksikin muuksi tietoturvatason kohottamiseksi. Mikäli tällä tavalla tehtäisiin, tulisi asennus dokumentoida erittäin hyvin ja pitää jatkossa mielessä tehdyt muutokset oletusasetuksiin.

3.8.2 Active Directoryn mahdolliset lisäpalvelut

AD DS:n peruspalveluiden lisäksi voidaan tarpeen mukaan ottaa käyttöön seuraavanlaisia palveluita, jotka laajentavat palvelimen palvelukonseptia:

Active Directory Certificate Services (AD CS)

Active Directory Certificate Services (AD CS) mahdollistaa varmenteisiin perustuvan julkisen avaimen infrastruktuurin rakentamisen. Tarjoaa mahdollisuuden käyttää salausta ja tunnistautumiseen esim. vahvaa sirukorttipohjaista järjestelmää käyttäen. Erinomainen ratkaisu tietoturvatason kohottamiseen. [4, s. 377] [17]

Active Directory Federation Services (AD FS)

Active Directory Federation Services (AD FS) mahdollistaa Single sign-on (SSO) eli kertakirjautumisen käyttöönoton järjestelmissä ja sovelluksissa, jotka ovat toisen organisaation hallinnoimia. [4, s. 421] [18]

Active Directory Lightweight Directory Services (AD LDS)

Active Directory Lightweight Directory Services (AD LDS) tarjoaa kevennetyn ratkaisun ja tuen hakemistokäyttöisille sovelluksille ilman AD:n riippuvuuksia. Ratkaisu ei tarjoa mahdollisuutta luoda toimialuetta, eikä ohjainkonetta. AD LDS voi toimia joko erillisenä tietovarastona tai replikoinnin kanssa. [19]

Active Directory Rights Management Services (AD RMS)

Active Directory Rights Management Services (AD RMS) avulla voidaan parantaa organisaation tietoturvaa, joka liittyy asiakirjojen suojaukseen ja käyttöoikeuksiin (IRM). [4, s. 459] [20]

DHCP-palvelin (Dynamic Host Configuration Protocol)

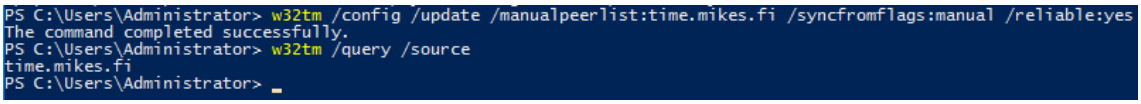
DHCP-palvelin jakaa IP-osoitteita ja muita verkkoasetuksia lähiverkon tietokoneille ja laitteille dynaamisesti. Palvelu helpottaa asiakaskoneiden verkkoasetuksien hallintaa. Tätä roolia ei välttämättä suositella asennettavaksi samaan koneeseen AD DS:n kanssa, vaan se voidaan asentaa erilliseen verkkolaitteeseen tai palvelimeen niin halutessaan. [21]

Tässä työssä ja tällä hetkellä ei otettu käyttöön muita lisärooleja, vaan selvisimme pitkälti Active Directoryn (AD DS) peruspalveluilla. Koko organisaation kattavissa ratkaisuissa kuitenkin usein tarvitaan monia lisärooleja palvelujen laajuudesta ja kriittisyydestä johtuen.

3.8.3 Palvelimen aika-asetukset

Active Directory on hyvin aikakriittinen, joten paikallisen ajan synkronointi oikean ja tarkan aikalähteen mukaan on tärkeää. Varsinkin laajoissa ja monen palvelimen ympäristössä voi syntyä toimintahäiriöitä, kuten kirjautumisen epäonnistumisia. AD sallii n. 5 min. epätarkkuuden, joten PDC-emulaattorin (Primary Domain Controller) aika on suositeltavaa synkronoida ulkoisen julkisen ja luotettavan aikalähteen eli NTP-palvelimen (Network Time Protocol) mukaan. Muiden toimialueen mahdollisten ohjainkoneiden aika synkronoidaan sitten PDC:n kellon mukaan [22]

Tässä työssä käytettiin PowerShellin komentotulkissa w32tm.exe-työkaluohjelmaa palvelimen ajan asettamiseen ulkoisen lähteen mukaan (time.mikes.fi, kuva 10):



Kuva 10. PDC-emulaattorin aikapalvelun synkronointi ulkoiseen NTP-palvelimeen

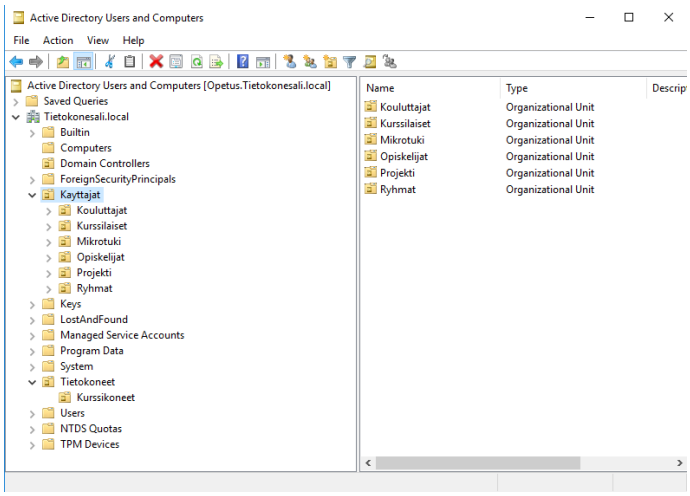
4 Active Directoryn hallintamallin rakentaminen

Active Directoryssa tiedot ovat tallennettu hierarkkisesti objekteihin. Objektit ovat määritteiden ryhmiä, jotka edustavat ko. alueen resurssia. Objekteille on määritetty yksilöllinen suojaustunniste (SID, Security Identifier). Suojaustunnistetta käytetään oikeuksien antamiseen tai kieltämiseen toimialueella. Tämän lisäksi objekteille annetaan maailmanlaajuinen yksilöllinen GUID-tunnistetieto (kohdassa 3.1 sivulla 7 on kerrottu GUID-tunnistetiedosta tarkemmin).

Toimialueen hallintamallia rakennettaessa tulee sinne tietyt tarpeelliset oletusobjektit. Organisaation oma hallintamalli rakennetaan samaan hierarkiaan. Active Directoryn hallintamallin loogisen suunnittelun pohjaksi otetaan usein organisaation todellinen reaalimaailmassa esiintyvä yrityksen organisaatiomalli. Hallintaoikeuksia voidaan näin ollen kätevästi delegoida organisaatioyksiköiden perusteella. AD:n hallintamalli voi rakentua myös organisaation eri toimipisteiden maantieteellisten sijaintien perusteella. Ryhmäkäytäntöjä (Group Policy) voidaan tällöin helposti kohdistaa eri organisaatioyksiköihin halutuilla tavoilla. Ryhmäkäytännöistä kerrotaan lisää kohdassa 4.2. sivulla 41.

4.1 Active Directoryn hallintatyökalu (ADUC)

Active Directoryn hallinta tapahtuu graafisesti ADUC-työkalulla (Active Directory Users and Computers). Se käynnistetään Server Managerin Tools -valikosta. Kuvassa 11 on kuvattuna esim. tietokonesalin hallintamalli. [4, s. 211]



Kuva 11. Tietokonesalin hallintamalli

Active Directoryn hallintamalliin rakennetaan oma halutunlainen hallintahierarkia. Organisaatioyksiköiden (Organizational Unit, OU) nimeämisessä on hyvä noudattaa johdonmukaisuutta ja selkeyttä. Saman nimisiä objekteja tulee välttää, ettei sekaannuksia syntyisi. Oletussäiliöihin **Users** ja **Computers** ei voi linkittää ryhmäkäytäntöjä, joten niitä ei kannata käyttää omassa hallintamallissa. Näihin oletussäiliöihin mahdollisesti ilmestyvät objektit tulee siirtää mahdollisimman nopeasti oikeisiin suunniteltuihin organisaatioyksikköihin.

Hallintamalliin luodaan käyttäjien hallintaan sopiva organisaatioyksikkö esim. **Kayttajat** (ei suositella skandeja). Tietokoneita varten luodaan **Tietokoneet** ja ryhmiä varten **Ryhmat**. Näiden organisaatioyksiköiden alle tulee muodostaa sopiva hierarkia riippuen omasta organisaation rakenteesta, laitekokoonpanosta ja käyttäjistä. **Tietokoneet**-yksikön alle voidaan luoda esim. **Tyoasemat** ja **Kannettavat**. Palvelimille kannattaa tehdä oma organisaatioyksikkönsä esim. **Palvelimet**. **Kayttajat**-yksikön alle voisi tulla esim. kuvan 11 kaltainen luokittelu. **Ryhmat**-yksikön alle voitaisiin koostaa kaikki käytössä olevat ryhmät. Suunnittelemalla hallintamalli huolellisesti selkeäksi ja loogiseksi rakenteeksi omasta organisaatiosta, helpottaa se jatkossa ylläpitäjän elämää. Toisaalta Active Directoryn rakennetta voi toki muokata myös jälkeenpäin, mikäli siihen tulee tarvetta.

4.1.1 Ryhmien ja käyttäjien lisääminen hallintamalliin

Ryhmät (Groups)

Ryhmiä käytetään oikeuksien ja vastuiden jakamiseen yleisesti organisaatioissa. Organisaatiossa esim. myynnillä ja huollolla on erityyppiset roolit ja tehtävät. Eri osastoilla on omat ja tietyt tietovarannot käytettävissään. Käyttöoikeudet tiedostoihin ja kansioihin voidaan helposti jakaa ryhmien avulla, eikä yksittäisille käyttäjille erikseen. Lisäämällä yksittäinen käyttäjä haluttuun ryhmään jäseneksi, saa tämä tällöin ryhmän kautta oikeudet tarvittaviin kansioihin ja tiedostoihin. Tätä menetelmää tulee käyttää aina kuin se on mahdollista ja välttää yksittäisille käyttäjille annettuja käyttöoikeuksia.

Active Directoryssa käytetään kahden tyyppisiä ryhmiä: **Security**- tai **Distribution**-tyyppisiä. Security-tyyppisiä ryhmiä käytetään käyttöoikeuksien hallintaan ja Distribution-tyyppisiä ryhmiä sähköpostin jakelulistojen määrittämiseen. [23]

Käyttäjäryhmää luodessa määritetään myös sen laajuus. Käyttäjäryhmät tukevat myös sisäkkäisiä ryhmiä (nested groups). Active Directoryn ryhmät luokitellaan niiden laajuuden mukaan: [4, s. 247]

- Domain Local Group
- Global Group
- Universal Group.

Domain Local Group: Voidaan käyttää yhden toimialueen resurssien ja oikeuksien hallintaan. Ainoa ryhmä, jossa voi olla jäseniä metsän ulkopuolelta. Voi sisältää tietokoneita, käyttäjiä, globaaleja ja universaaleja ryhmiä mistä tahansa metsän toimialueesta ja mistä tahansa luotetusta toimialueesta. Voi sisältää myös saman toimialueen paikallisia ryhmiä ja olla niissä jäsenenä. Tätä ryhmää käytetään pääsääntöisesti resurssien ja käyttöoikeuksien hallintaan kaikkialla toimialueella.

Global Group: Voi sisältää tietokoneita, käyttäjiä ja ryhmiä samasta toimialueesta, mutta ei universaaleja ryhmiä. Se voi olla saman toimialueen globaalien ryhmien ja paikallisten ryhmien jäsen. Se voi olla jäsenenä minkä tahansa samassa metsässä olevan toimialueen universaalissa ryhmässä tai luotetussa toimialueessa. Tätä ryhmää käytetään toimialueen kokoelmia luodessa, jotka ovat roolipohjaisia, kuten esim. organisaation HR-, myynti- ja huoltoyksikkö.

Universal Group: Universaali ryhmä ei välitä toimialueiden luottamussuhteista. Voi sisältää käyttäjiä ja ryhmiä globaaleista sekä universaaleista ryhmistä metsän mistä tahansa toimialueesta. Universaalit ryhmät voivat olla toimialueen paikallisten ryhmien tai muiden universaalien ryhmien jäseniä, mutta ei globaalien ryhmien jäseninä. Tätä ryhmää ei kannata käyttää yhden toimialueen ratkaisussa.

Käyttäjät (Users)

Ennen kuin päästään lisäämään käyttäjiä AD:n hallintamalliin, tulisi ymmärtää pari seikkaa liittyen käyttäjäobjektin attribuutteihin. Tärkeimmät attribuutit kirjautumisen kannalta ovat: **samAccountName** ja **UserPrincipalName (UPN)**. [24]

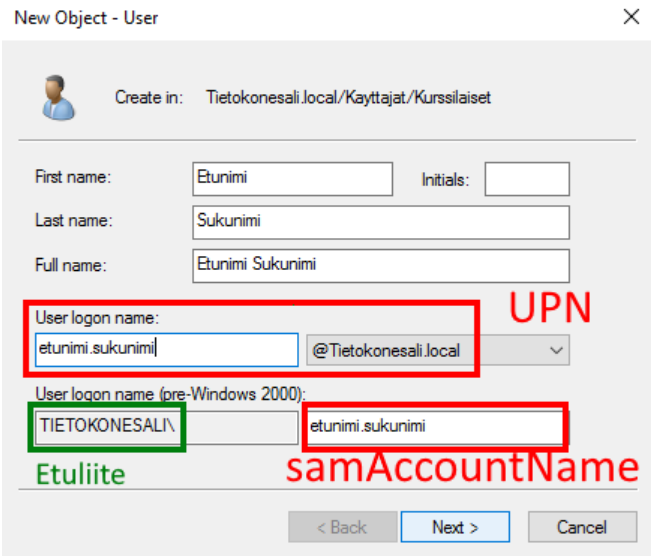
samAccountName

samAccountName attribuuttia käytettiin Windows NT toimialuekirjautumiseen ennen Windows 2000 ympäristön tuloa. Attribuuttia käytetään edelleen kirjautumisessa toimialueeseen ja valtuutukseen. Sen muoto on kuvassa 12 esitetyn kaltainen toimialueennimi\tunnus. Tämä kirjautuminen käyttää lähiverkkoprotokollaa (NetBIOS ja NetBEUI). Tunnuksen tulee olla yksilöllinen toimialueessa. Sen maksimipituus on 20 merkkiä. Nykyisin tarvitaan kuitenkin myös internet-muotoinen tunnus (UPN, User Principal Name), joka toimii myös DNS-hierarkkisessa verkossa. [25]

UserPrincipalName (UPN)

Windows 2000 tulon myötä alettiin käyttämään hakemistopalvelussa LDAP-yhteysprotokollaa, joka käyttää DNS-nimiä hierarkkisena organisaatiorakenteena.

Hakemistopalvelussa käyttäjätilit tunnistetaan yksilöllisesti UserPrincipalName (UPN) -kirjautumisnimien perusteella (kuva 12). UPN on sähköpostimuotoinen ja perustuu RFC 5322 standardiin. Sen ei tarvitse olla kuitenkaan käyttäjän sähköpostiosoite, vaan se riippuu toimialueen rakenteesta. Sen maksimipituus on 256 merkkiä. [25]



Kuva 12. Kirjautumisattribuutit

Käyttäjätunnuksen luonti

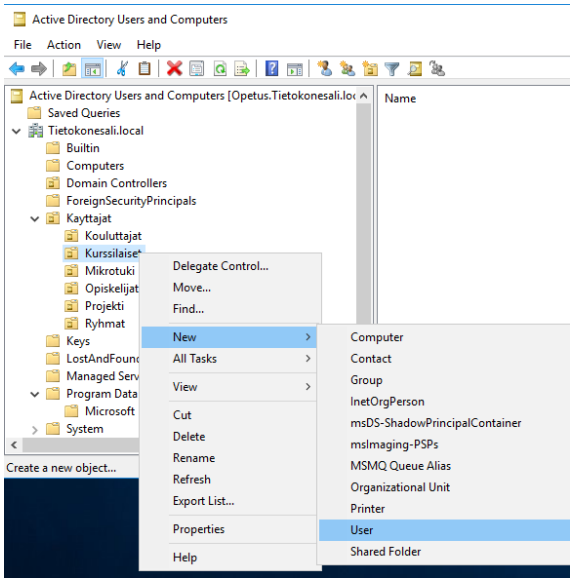
Käyttäjien lisääminen tapahtuu, joko manuaalisesti tai jollakin automatiikalla esim. skripteillä. Jos on kysymys suurista määristä käyttäjiä, niin tunnuksia voidaan luoda erillisillä skripteillä automaattisesti tai puoliautomaattisesti lähdetietojen perusteella. Usein käytetään skriptauskielenä Windowsin kehittynyttä PowerShell-komentotulkkia Windows-järjestelmien ylläpitotehtävissä sen monikäyttöisyyden vuoksi.

Seuraavissa kuvissa (13-15) näytetään esimerkkinä käyttäjän lisääminen manuaalisesti graafisella Active Directoryn ADUC-hallintatyökalulla:

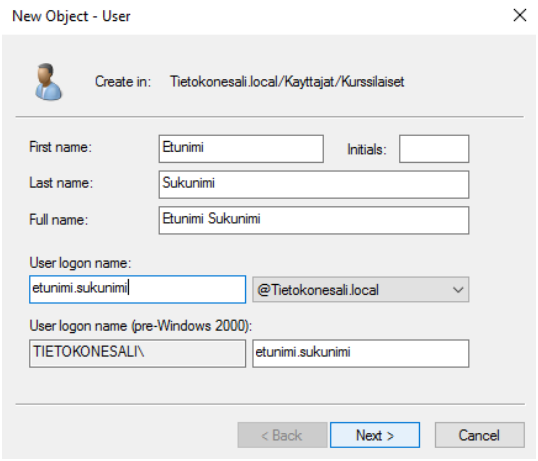
Klikataan hiiren oikealla painikkeella halutun organisaatioyksikön (Kurssilaiset) päällä ja valitaan **New->User** (kuva 13). Täytetään kentät siten, että luotava

käyttäjätunnus on yksilöllinen ja usein käytetään **etunimi.sukunimi**-muotoista mallia käyttäjätunnuksissa, kuten kuvassa 14 esitetään. Seuraavaksi edetään väliaikaisen salasanan luontiin, joka on syytä olla kohtuullisen tietoturvallinen (väh. 16 merkkiä), jonka käyttäjä sitten vaihtaa halutuksi mahdollisimman nopeasti (kuva 15). Hyväksytään lopuksi kuittaamalla.

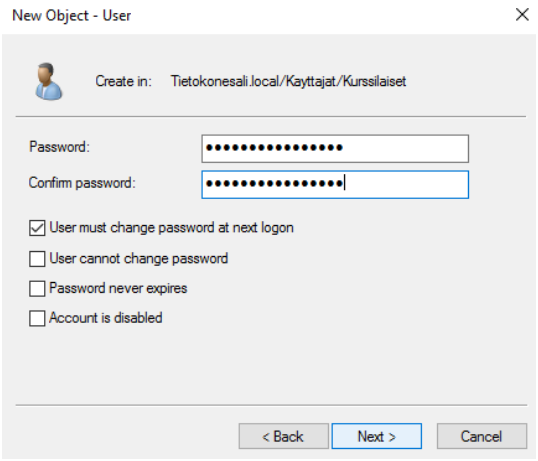
Tämän jälkeen muokataan käyttäjän muita ominaisuuksia **Ominaisuudet**-valinnan kautta (kuva 14). Suurin osa tarvittavista ja yleisimmistä käyttäjän määritteistä löytyvät **Account**- ja **Profile**-välilehdistä. Niitä ovat mm. tilin vanhentumisajan-kohta, tilin salasanamääreet, tilin käyttöön liittyvät rajoitukset, kotikansion polkumääritys, skripteihin liittyvät määritykset jne.



Kuva 13. Käyttäjän lisääminen Active Directoryyn



Kuva 14. Uuden Käyttäjäobjektin luonti



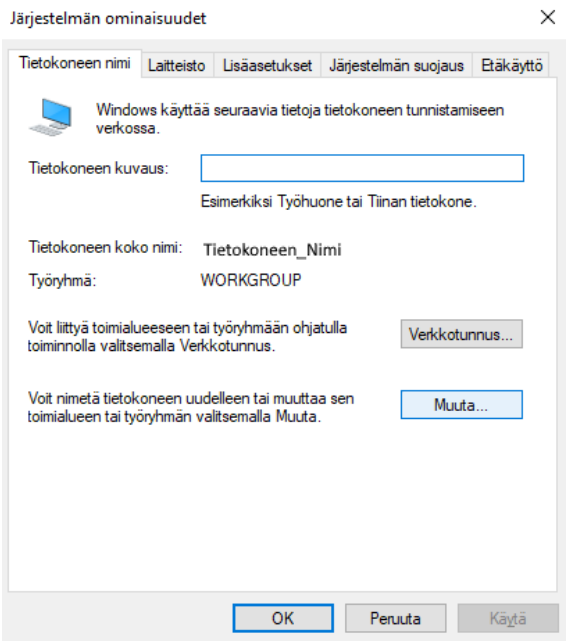
Kuva 15. Salasanan asettaminen väliaikaisesti käyttäjälle

4.1.2 Työaseman liittäminen toimialueeseen

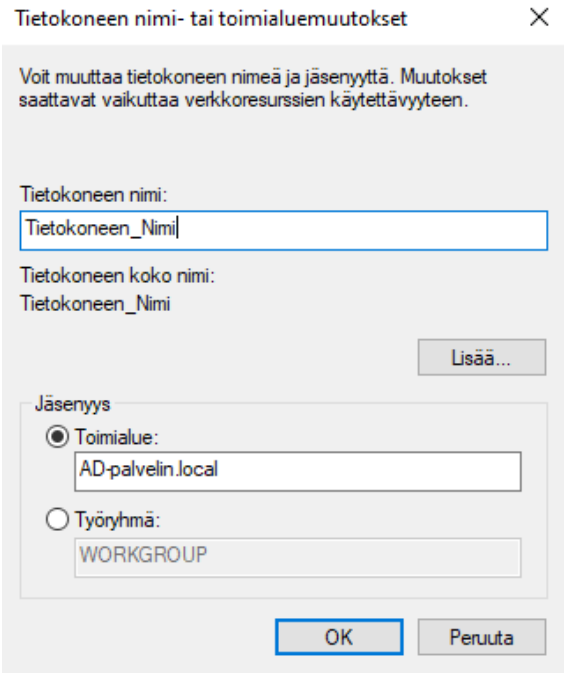
Yksittäiset työasemat liitetään usein työasemalta käsin manuaalisesti toimialueeseen. Mikäli työasemia on paljon, niiden liittäminen AD:hen voidaan automatisoida esim. PowerShell-skriptillä, joka hakee esim. tekstitiedostosta tarvittavat tiedot liitettävistä koneista. Ennen työaseman liittämistä toimialueeseen esimerkin mukaisesti tulee se nimetä loogisella ja kuvaavalla nimellä. Tämä siksi, että ylläpitäjät voisivat jatkossa paikallistaa työaseman lähiverkossa sekä toimialueen hallintamallissa. Työaseman nimeämiseen tarvitaan paikallisen työaseman pääkäyttäjän oikeuksia ja useiden työasemien (>10) liittämiseen toimialueeseen

tarvitaan esim. toimialueen Domain Admins -tason tunnukset, joten ne tulee olla käytettävissä ennen työaseman tai työasemien liittämistä toimialueeseen. Toimialueen peruskäyttäjä voi oletusarvoisesti liittää 10 tietokonetta toimialueeseen.

Manuaalinen liittäminen työasemalla tehdään: **Järjestelmän lisäasetuksista**. **Tietokoneen nimi** -välilehdeltä klikataan painikkeesta **Muuta…**, kuten kuvassa 16 esitetään. Tämän jälkeen Jäsenyys-kohtaan valitaan **Toimialue**: ja kenttään kirjoitetaan **toimialueen nimi** (kuva 17), jonka jälkeen toimialue pyytää käyttäjätunnusta, jolloin käytetään esim. toimialueen käyttäjätunnusta. Onnistuneen liitoksen jälkeen työasema käynnistetään uudestaan.



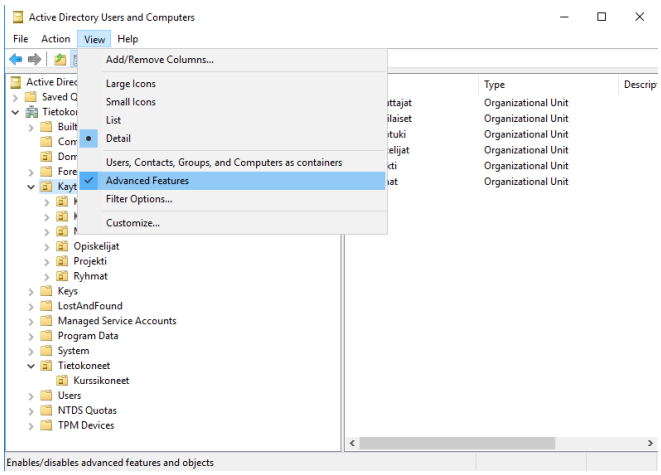
Kuva 16. Työaseman nimi-välilehti



Kuva 17. Työaseman liittäminen toimialueeseen

ADUC ja Advanced Features

ADUC-työkalun käyttöliittymän näkymää voi vaihtaa tarkempaan esitysmuotoon View-valikosta valitsemalla **Advanced Features** valituksi, jolloin kaikki AD:n objektit tulevat näkyviin ja kaikkiin mahdollisiin parametreihin pääsee tarvittaessa käsiksi (kuva 18). Tätä laajennettua näkymää käytetään, mikäli ei löydetä haluttua objektia tai asetusta hallintamallista. Huomioitavaa tässä vaiheessa kuitenkin on se, että varomaton parametrien muokkaaminen voi johtaa vakaviin häiriöihin järjestelmän toiminnassa. [26]



Kuva 18. ADUC:n laajennetun näkymän valinta

4.2 Ryhmäkäytännöt (Group Policy, GP)

Ryhmäkäytäntöobjekteilla (GPO, Group Policy Object) voidaan määritellä keskitetysti monia sääntöjä, asetuksia, suojauksia, käyttöoikeuksia sekä toimintoja tietokoneille ja käyttäjille toimialueella. Ryhmäkäytäntöjen avulla voidaan myös asentaa ohjelmia ja ajaa komentojonoja sekä skriptejä. Ryhmäkäytäntöjen käyttöönotossa tulee olla erityisen huolellinen ja ne tulee testata ja dokumentoida hyvin. [4, s. 279]

Ryhmäkäytäntöjen nimeämisessä on syytä käyttää mahdollisimman hyvin kuvaavia nimiä käyttötarkoituksen mukaan. Tehtäväkohtaiset ryhmäkäytännöt ovat usein suositeltavia. Tällöin tehdään juuri tiettyyn tehtävään tarkoitettu ryhmäkäytäntö esim. Tietokoneiden päivitys (Windows_Update) tai Kansioiden jako (Map_Drive).

Ryhmäkäytäntöjä (GP) voidaan määritellä hallintamallin eri hierarkian tasoille haluttuun organisaatioyksikköön (OU). Ryhmäkäytännöt prosessoidaan eli ajetaan seuraavassa järjestyksessä:

- paikalliset ryhmäkäytännöt
- toimipaikan ryhmäkäytännöt
- toimialueen ryhmäkäytännöt

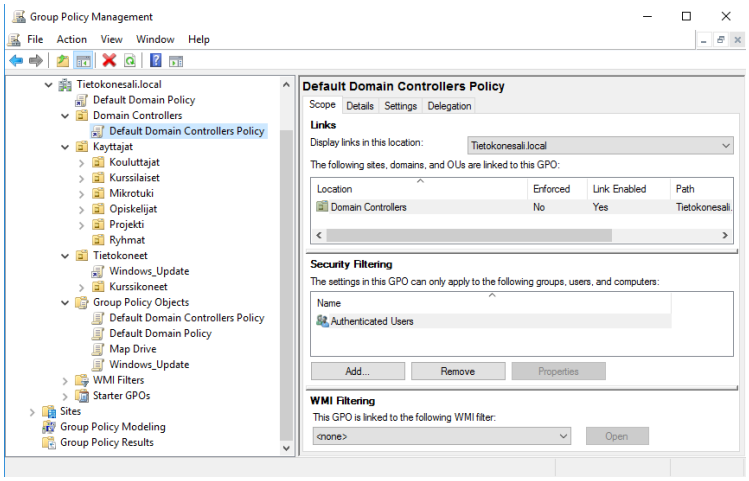
- organisaatioyksikön ryhmäkäytännöt.

Viimeisenä prosessoitu vaikuttava ryhmäkäytäntö jää voimaan, ellei sitä ole erikseen estetty. Linkitetyt ryhmäkäytännöt vaikuttavat kaikkiin objekteihin, jotka ovat linkitetyn objektin hierarkian alla. Ryhmäkäytäntöjä ei voi linkittää **Computers**- ja **Users**-oletussäiliöihin, joten sinne ilmaantuvat objektit tulee siirtää haluttuihin organisaatioyksikköihin.

Ryhmäkäytännöt päivittyvät oletusarvoisesti 90 minuutin välein. Muokatut ryhmäkäytännöt voidaan pakottaa voimaan heti **gpupdate**-komennolla komentotulkissa tai käynnistämällä kohteena ollut työasema uudelleen, johon määritteet kohdistuvat. Nämä kannattaa huomioida ryhmäkäytäntöjen muokkauksissa ja testauksissa. [27]

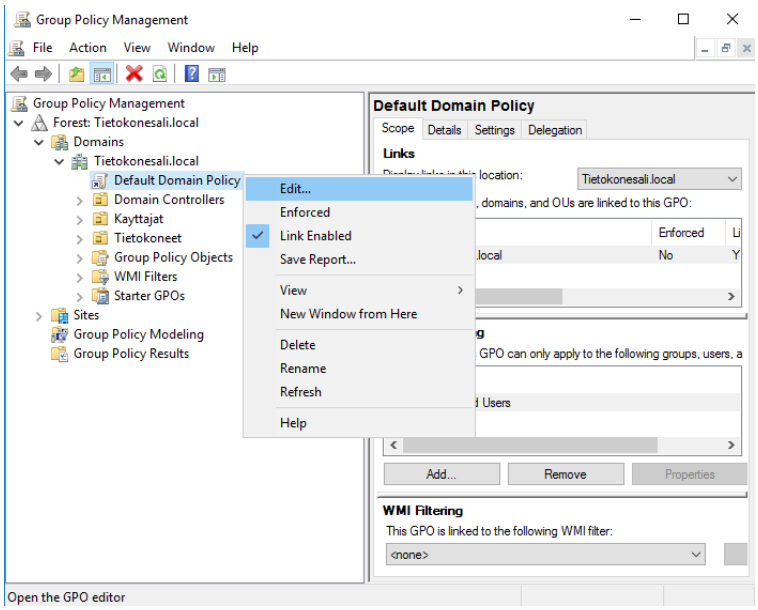
Ryhmäkäytännön muokkaaminen

Ryhmäkäytäntöjen työkalu löytyy **Server Managerin Tools** -valikosta valitsemalla **Group Policy Management**. Kuvassa 19 näkymä toimialueen oletusryhmäkäytännöistä. Kaikki toimialueen ryhmäkäytännöt näkyvät Group Policy Objects -haarassa.



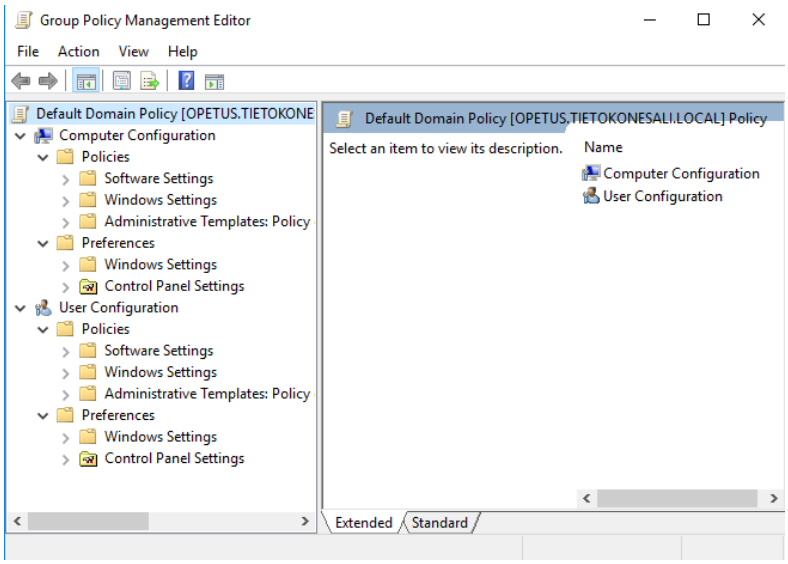
Kuva 19.Toimialueen oletusryhmäkäytäntö

Toimialueen oletusryhmäkäytäntöön (Default Domain Policy) on määritelty koko toimialuetta koskevia oletusasetuksia. Olemassa olevaa oletusryhmäkäytäntöä ei suositella yleensä muokattavaksi. Tälle tasolle voisi korkeintaan laittaa esim. suojauksiin ja salasanakäytänteisiin liittyviä koko toimialuetta koskevia määritteitä. Tässä esimerkissä esitetään periaate, miten muokkaus voitaisiin käytännössä aloittaa, mikäli näin haluttaisiin tehdä. Käynnistetään Group Policy Management -työkalu ja sen jälkeen hiiren oikealla painikkeella klikkaamalla halutun ryhmäkäytännön päällä. Valitsemalla **Edit**-tila valikosta päästään eteenpäin, kuten kuvassa 20 esitetään.



Kuva 20. Default Domain Policyn muokkaus

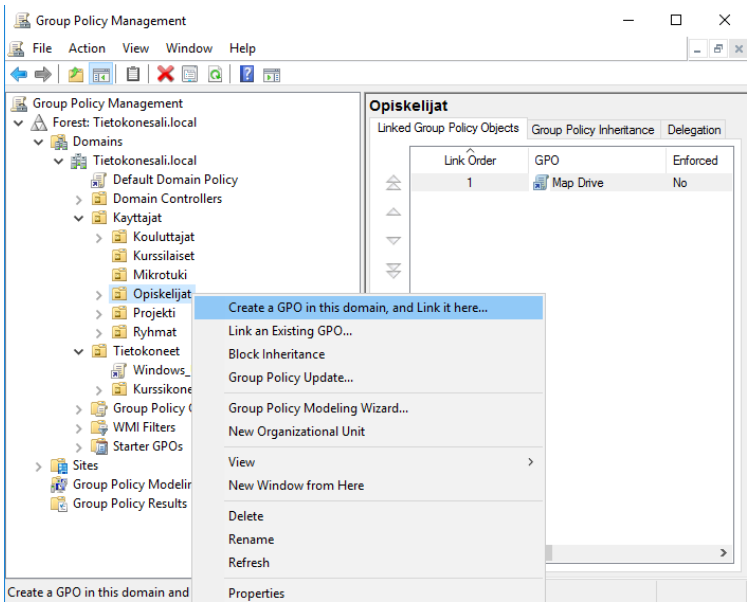
Kuvassa 21 näkyvät varsinaisessa ryhmäkäytännön editointitilassa kaksi päähaaraa: **Computer Configuration** ja **User Configuration.** Näiden päähaarojen alle voidaan tehdä määrityksiä liittyen toimialueen oletusryhmäkäytäntöön, toisaalta näin laajalle vaikutusalueelle vaikuttavan oletusryhmäkäytännön muokkaus tulee tehdä harkiten. Huomioitavaa on se, että tähän kohtaan linkitetty ryhmäkäytäntö vaikuttaa kaikkiin ko. toimialueen tietokoneisiin ja käyttäjiin. Ryhmäkäytäntöjä kannattaa yleensä käyttää pääsääntöisesti alemmilla OU-tasoilla.



Kuva 21. Group Policy Management Editor

Uuden ryhmäkäytännön luominen

Uuden ryhmäkäytännön luominen aloitetaan esimerkiksi halutussa organisaatiohaarassa (**Create a GPO in this domain and Link it here…**), kuten kuvassa 22 esitetään. Siinä ryhmäkäytännön vaikutus kohdistuu esim. Opiskelijat-organisaatioyksikköön ja sen alla oleviin käyttäjiin.



Kuva 22. Uuden ryhmäkäytännön luominen

Windows update -ryhmäkäytännön luonti työasemille

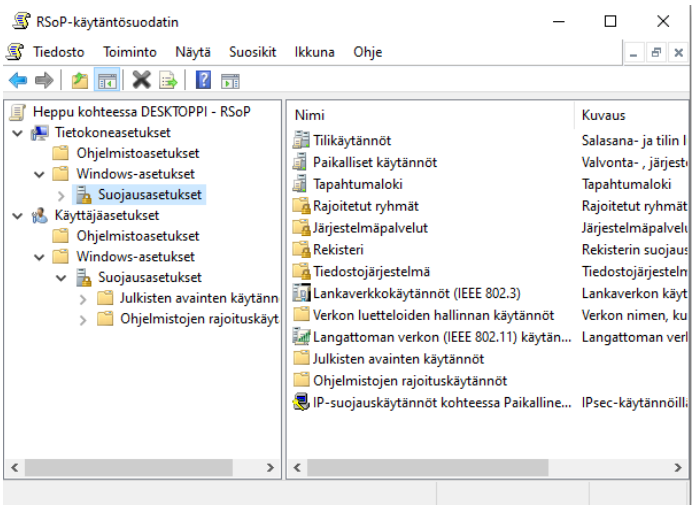
AD-palvelimelle omaan hallintamalliin voidaan esimerkiksi luoda tietokoneluokan työasemille sopiva ryhmäkäytäntö, joka määrittelee, miten Windows-päivitykset ajetaan työasemilla. Luodaan Windows-päivityksiä varten erillinen ryhmäkäytäntö nimeltään Windows_Update. **Liitteessä 1** esitetään miten **Windows_Update** -ryhmäkäytäntö on muodostettu.

4.3 Ryhmäkäytäntöjen tarkistustyökalut työasemilla

RSoP- ja **GPResult**-työkaluilla voidaan tutkia mitkä ryhmäkäytännöt ovat voimassa työasemalla. Molempia työkaluja suoritetaan komentorivitulkissa eli komentokehotteessa ja ne vaativat usein paikallisen tietokoneen pääkäyttäjän oikeuksia. [4, s. 728]

RSoP.msg-työkalu (Resultant Set of Policy)

RSoP-työkalu kerää paikallisen työaseman tietokonekohtaiset vaikuttavat ryhmäkäytännöt ja näyttää tiedot ikkunassa, kuten kuvassa 23 esitetään. Tämä työkalu ei näytä kaikkia ryhmäkäytäntöjä vaan ainoastaan tietokonekohtaiset. Komento kirjoitetaan komentorivitulkissa muodossa: **rsop.msg.** [27]



Kuva 23. Rsop-työkalun käyttö työasemalla

GPResult.exe-työkalu (Group Policy Result Tool)

GPResult.exe-komentorivityökalu näyttää kaikki voimassa olevat ryhmäpolitiikat työasemalla (tietokoneen ja käyttäjän), mutta se näyttää tulokset komentorivitulkissa, eikä avaa graafista ikkunanäkymää. Tämä työkalu on erittäin käyttökelpoinen työkalu järjestelmän pääkäyttäjille. [28]

gpresult /r

Gpresult vaati lisäparametrin /r, jotta se näyttää yhteenvedon kaikista vaikuttavista ryhmäpolitiikan tiedoista. Lisätietoja komennosta saadaan parametrillä **/?**

gpresult /r /scope:user

Näyttää käyttäjäkohtaiset vaikuttavat ryhmäpolitiikat.

gpresult /r /scope:computer

Näyttää tietokonekohtaiset vaikuttavat ryhmäpolitiikat

gpresult /h c:\reports.html

Yllä oleva komento luo graafisen raportin kaikista vaikuttavista työaseman ja käyttäjän ryhmäkäytännöistä sekä tallentaa reports.html nimisen tiedoston C:-levyn juureen. Tiedoston tallennus juurikansioon vaatii paikallisen pääkäyttäjän oikeudet. Tiedosto on luettavissa esim. internet-selaimella.

GPUpdate-komento

Tämän lisäksi käyttökelpoisiksi työkaluiksi ovat osoittautuneet komennot:

gpupdate

gpupdate /force

Näillä komennoilla voi päivittää tai suorittaa pakotetusti työasemalla kaikki käyttöön tulevat ryhmäkäytännöt heti voimaan, jolloin asetuksien testaus nopeutuu.

Ryhmäkäytäntöjen oletuspäivitysväli on 90 minuuttia, joten tämä työkalu nopeuttaa esim. niiden testaamista. [29]

4.4 Kansioiden ja tiedostojen jakaminen

Organisaation tietovarannot eli kansiot ja tiedostot voivat tänä päivänä sijaita missä vain, joko paikallisesti omalla tiedostopalvelimella tai ns. ”pilvessä” eli jossain muualla verkossa olevalla kenties ulkoisella tiedostopalvelimella (esim. Microsoftin One Drive). Yhä käytetään toki vielä paikallisia tallennusmedioita tilanteen niin vaatiessa. Tiedostoja tallennetaan myös työaseman paikalliselle kiintolevylle tai muistikortille, näin toimitaan usein kotikoneissa. Suosituin tapa nykyisin kuitenkin lienee se, että kansiot ja tiedostot tarjotaan verkon kautta käyttäjälle. Varmistukset tiedostoista otetaan hyvin usein johonkin turvalliseen pilvipalveluun, jolloin ne ovat tallessa, vaikka päätelaite jostain syystä rikkoontuisi tai katoaisi.

Organisaatiot ottavat usein käyttöön tähän tarkoitukseen suunniteltuja verkkolevypalvelimia eli *Network-attached storage (NAS)* -palvelimia. NAS-levypalvelimet ovat yleensä Linux-pohjaisia tiedoston tallennusjärjestelmiä, joita käytetään pääsääntöisesti lähiverkoissa ja jopa ulkoverkoissa (suojaukset ja salaukset). NAS-levypalvelimia hankkivat pienet ja keskisuuret yritykset, tosin löytyy niitä järeitäkin malleja, jotka soveltuvat myös suuryrityksillekin.

Suuryritykset rakentavat usein puolestaan valtavia varastointiverkkoja, jotka perustuvat taas *Storage Area Network (SAN)* -tekniikkaan. Näissä kaikissa tallennustekniikoissa on huomioitava verkon toimivuus eri tilanteissa ja varmistuttava tiedonsiirron sekä tallennuksen tietoturvallisuudesta. Tiedostojen säilyttäminen ja jakaminen käyttäjille on tehtävä riittävän tietoturvallisella tavalla ottaen huomioon tietojen kriittisyysluokittelu. [30]

4.4.1 Tiedostopalvelimet

Tiedostopalvelimet ovat erittäin tärkeässä ja kriittisessä roolissa organisaation ICT-palveluissa. Niiden kriittisyysaste lienee samaa luokkaa Active Directoryn

palveluiden kanssa. Siksi varsinaisiin tiedostopalvelimiin ei suositella asennettavaksi muita rooleja tai palveluita kuin tiedostojen hallintaan liittyviä. Tallennusmedioiden vikasietoisuus tulee olla korkealla tasolla ja varmistukset kunnossa. Tiedostojen varmistukset tulee tehdä tietoturvallisesti erillisellä automatisoidulla proseduurilla esim. ulkoiselle turvalliselle medialle. Varmistukset tulisi salata tarvittaessa ja niitä on säilytettävä turvallisessa sijainnissa. Tärkeimpien tietojen osalta varmuuskopioiden tallennuspaikkoja tulisi olla vähintään kahdessa eri fyysisessä sijainnissa.

Server Message Block (SMB) -verkon viestintäprotokolla

IBM:n 1980-luvulla alun perin kehittämä verkkoviestintäprotokolla SMB (Server Message Block) on yksi suosituimmista ratkaisusta tiedostojen jakamiseen palvelimissa ja lähiverkoissa. SMB-protokollasta on ajan saatossa kehitetty erilaisia paranneltuja muunnelmia. Tällä hetkellä SMB-protokollasta on suositeltavaa käyttää mahdollisimman uusinta 3.x-versiota, joka on tällä hetkellä tietoturvallisin. Nykyisin SMB-protokolla toimii suoraan TCP/IP:n päällä ja käyttää porttia 445. Windows Server 2016 -käyttöjärjestelmä tukee myös uusinta SMB 3.1.1-versiota. [31]

New Technology File System (NTFS) -tiedostojärjestelmä

NTFS-tiedostojärjestelmä on Microsoftin kehittämä tiedostojärjestelmä, jonka ensimmäinen versio esiteltiin jo vuonna 1993. Versio 3.1 on nykyisin ensisijaisena tiedostojärjestelmänä Windows-käyttöjärjestelmien sisäisissä levyissä. NTFS-tiedostojärjestelmä on tehokas, tietoturvallinen, monipuolinen ja kohtuullisen yhteensopiva muiden käyttöjärjestelmien kanssa. NTFS-tiedostojärjestelmän monipuolisiin ominaisuuksiin kuuluu nykyisin mm. [32]

- journalointi
- pitkät tiedostonimet (Windows rajoittaa nimen 259 merkkiin)
- käyttöoikeuksien hallinta
- salaus

- käyttäjäkohtaiset levytilat
- suurten levyjen tuki (256TB-8PB)
- ei tiedoston kokorajoitusta
- osioiden muokkausmahdollisuus.

NTFS-käyttöoikeudet

Microsoft Windows-käyttöjärjestelmässä on kaksi tapaa hallita ja rajoittaa käyttöoikeuksia: *NTFS-käyttöoikeudet* (suojaus) ja *jaetun resurssin käyttöoikeudet* (jakaminen). NTFS-käyttöoikeuksia käytetään kaikissa palvelimen levyaseman kansioissa ja tiedostoissa, jotka on alustettu NTFS-tiedostojärjestelmään. NTFS-käyttöoikeudet ovat voimassa paikallisesti palvelimella sekä käytettäessä etänä jaettuja resursseja. Käyttöoikeudet periytyvät oletusarvoisesti yläkansiosta alikansioihin, ellei periytymistä katkaista. Perustason käyttöoikeudet ovat:

- täydet oikeudet
- muokkaa
- lue ja suorita
- näytä kansion sisältö
- lue
- kirjoita.

Lisäkäyttöoikeuksilla voidaan ottaa kantaa käyttöoikeuksiin yksityiskohtaisemmin mm:

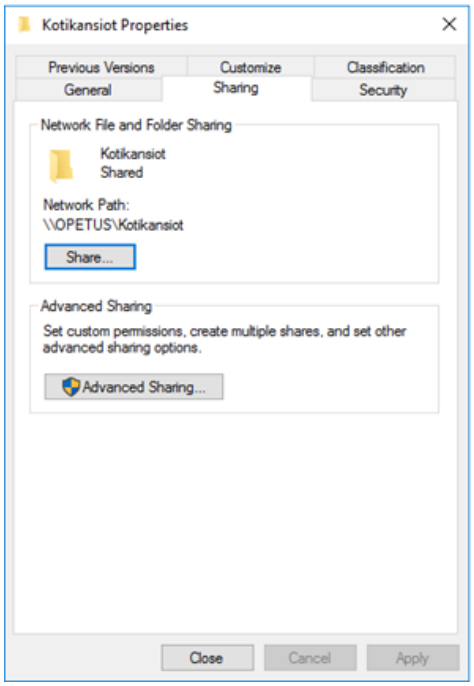
- käy kansio läpi tai suorita tiedosto
- luetteloi kansion sisältö / lue tiedot
- lue määritteet
- lue lisämääritteet
- lue tiedostot / kirjoita tiedot
- luo kansiot / liitä tiedot
- kirjoita määritteet
- kirjoita lisämääritteet
- poista alikansiot ja tiedostot

- poista
- lukuoikeudet
- muutosoikeus
- ota omistukseen.

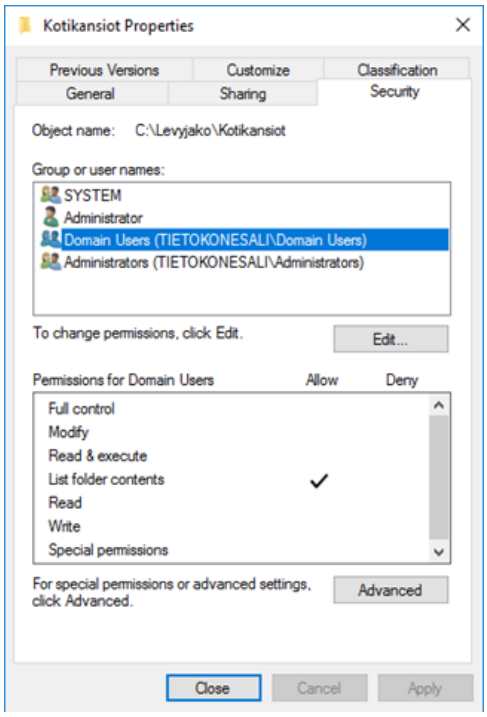
Jaetuissa kansioissa käytetään jaetun resurssin käyttöoikeuksia. Käyttöoikeudet ovat voimassa, silloin kun jaettuja kansioita ja tiedostoja käytetään verkon kautta etäkoneella. Käyttöoikeuksia on tarjolla tällöin kolme kpl:tta:

- täydet oikeudet
- muokkaus oikeudet
- lukuoikeudet.

Kansioita ja tiedostoja jaettaessa käyttöoikeuksia rajoitetaan molemmilla tavoilla eli jaetun resurssin käyttöoikeuksilla ja NTFS-käyttöoikeuksilla. **Eniten rajoittavat käyttöoikeudet ovat tällöin voimassa**. Jako- ja NTFS- käyttöoikeudet voidaan määrittää kansion tai tiedoston ominaisuudet-ikkunassa, kuten kuvista 24 ja 25 näkyy.



Kuva 24. Jakaminen-välilehti



Kuva 25. NTFS-käyttöoikeuksien asettaminen kansioon

Volume Shadow Copy Service (VSS)

Volume Shadow Copy Service (VSS), joka tunnetaan myös nimellä Volume Snapshot Service -palvelu, on ollut Windows Server 2003 lähtien käytettävissä Windows-käyttöjärjestelmissä. Levyaseman tilannevedospalvelu (snapshot) palvelimella luo varmuuskopioita tai varjokopioita tiedostoista haluttuun tallennuspaikkaan halutun aikataulun mukaisesti. Varjokopioita tehdään määritetyllä tavoilla tiedostoista, vaikka ne olisivat käytössä. Mikäli käyttäjä esim. poistaa epähuomiossa tiedoston, niin se on palautettavissa aikaisemmin tehdystä varjokopiosta, vaikkapa kesken työpäivän.

VVS-palvelu kannattaa yleensä laittaa päälle esim. käyttäjien kotikansioihin, jotka sijaitsevat omalla levytaltiollaan. Tämä tuo lisäturvaa tiedostoille, mutta ei korvaa varsinaista varmuuskopiointia. Varmuuskopiointiohjelmat käyttävät VSS-palvelua hyväkseen tehdessään varmuuskopiointia, jolloin tiedostot voidaan varmuuskopioida, vaikka tiedostot olisivat käytössä samanaikaisesti. [33]

Distributed File System (DFS)

Microsoftin tarjoama koko organisaatiota kattavista tiedostojärjestelmistä mainittakoon hajautettu tiedostojärjestelmä Distributed File System (DFS). Tiedostot ja kansiot voivat sijaita useilla eri palvelimilla, jotka sijaitsevat vaikkapa eri paikkakunnilla tai eri kiinteistössä. Käyttäjälle tiedostot ja kansiot näkyvät ikään kuin normaalina paikallisena resurssina. DFS-järjestelmää on käytetty yleensä vain lähiverkoissa. Nykyisin on kuitenkin mahdollista operoida myös internetin kautta uusilla tekniikoilla. [34]

Nykyisin organisaatioiden eri hybridimallien vallitessa myös tiedostojen salausjärjestelmien käyttöönottoa kannattaa harkita. Tämä siksi, koska organisaation sisäverkkoa ei voida enää suojata ulkoisilta uhkilta siinä määrin kuin ennen. Tämä siksi, koska moninaisten ulkoisten pilvipalveluiden käyttöönotto vaatii rajapintojen avaamista ulkoverkkoon. Suuntauksena näin ollen on se, että kaikki kriittiset tiedot ja tiedostot on salattava oletusarvoisesti, koska tänä päivänä ei ole olemassa turvallista ja eristettyä sisäverkkoa. Tämän lisäksi käyttäjien moninaiset mobiililaitteet asettavat pääkäyttäjille ja tietoturvan ylläpitäjille melkoisen lisähaasteen.

4.4.2 Tiedostopalvelun käyttöönotto palvelimessa

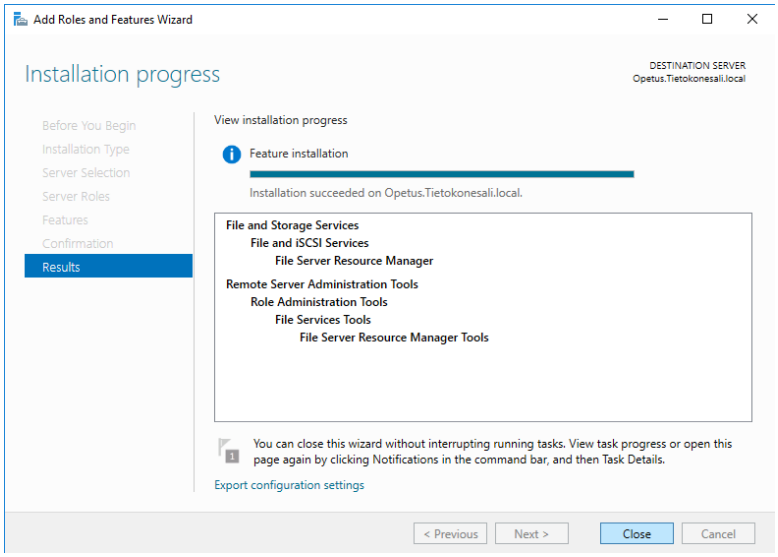
Tässä tehtävässä kehitystyössä riittää kuitenkin perustason lähestymiskulma tiedostopolitiikkaan. Työssä käytetään ainoastaan yhtä fyysistä palvelinta kaikkiin opetusympäristössä tarvittaviin AD:n peruspalveluihin ja tiedostopalveluihin. Tämän tyyppinen ratkaisu ei ole kovin järkevä ja suositeltava vaihtoehto pidempiaikaisiin ja laajempiin ratkaisuihin organisaatioissa.

Tiedostot tulisi säilöä omalla levyllään eikä samalla kuin palvelimen käyttöjärjestelmä. Paras vaihtoehto tiedostojen tallennuspaikkana lienee siihen tarkoitukseen rakennettu erillinen järjestelmä tai palvelin. Tässä opetusympäristössä ja käyttötarkoituksessa yhden palvelimen järjestelmä on kuitenkin riittävä huomioiden kaikki tietoturvaan liittyvät seikat. Toisaalta mahdollisesti kehitystyön

jatkosuunnitelmiin kuuluu uuden palvelimen hankkiminen, jolloin tiedostopalvelut voitaneen toteuttaa oikeaoppisesti ja tietoturvallisemmin.

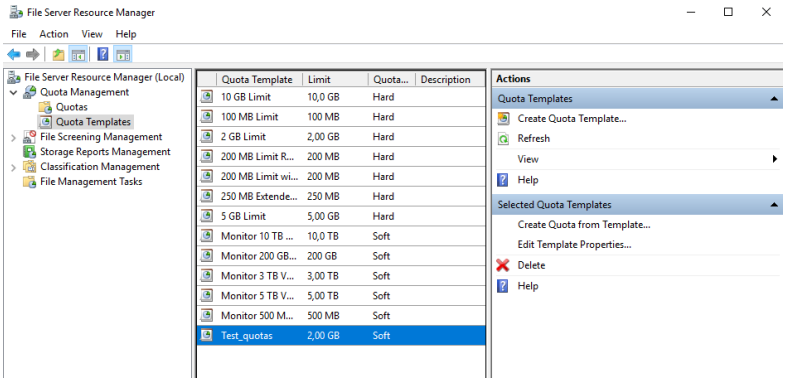
Tiedostopalvelun asennus palvelimeen

Palvelimeen lisätään tarvittavat palvelut (roolit ja ominaisuudet) palvelimen hallintaikkunan (Server Manager) kautta kohdasta Lisää rooleja ja ominaisuuksia (Add roles and features). Huomioitavaa on se, että Active Directoryn asennuksen yhteydessä asennettiin valmiiksi myös tiedostojen jakoon liittyvät peruspalvelut. Suositeltavaa kuitenkin on ottaa lisäksi käyttöön **File Server Resource Manager (FSRM)** -lisäominaisuus, kuten kuvassa 26 esitetään.



Kuva 26. File Server Resource Managerin asennus

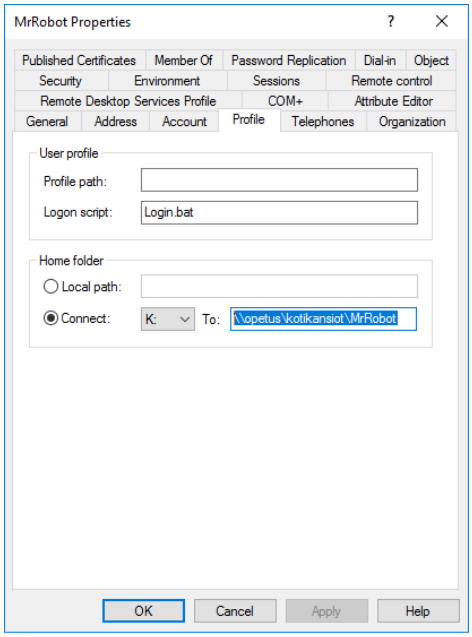
FSRM:n asennus palvelimeen tuo lisää tarkempia määritysmahdollisuuksia tiedostojen ja kansioiden hallintaan. Sen avulla saadaan hyödyllisiä tiedostoraportteja tiedostovarannoista. Palvelun voidaan luoda esim. eri levykiintiöitä käyttäjille ja asettaa hälytyksiä, mikäli rajat ylittyvät. Palvelusta löytyy valmiita mallipohjia (Templates) levykiintiöiden luomiseen ja näitä mallipohjia voi muokata halutunlaisiksi. Kuvassa 27 näkyy valmiita levykiintiömalleja, joita voi hyödyntää tai tehdä niistä tarvittaessa omat levykiintiömääritykset. File Server Resource Manager käynnistetään Tools-valikosta. [35]



Kuva 27. FSRM-levykiintiöiden oletusmallit (Templates)

Jakokansioiden luominen ja käyttöoikeuksien määrittely

Tiedostopalveluiden asennuksen jälkeen suunniteltiin kansioiden ja tiedostojen jaot käyttäjille. Tässä työssä suunnitelmana on tarjota käyttäjille omat kotikansiot (K:-asema) ja yhteinen kansio (M:-asema) koulutusmateriaalin jakamiseen. Kotikansion eli K-aseman linkitys (ns. ”mäppäys”, eng. map-sanasta) käyttäjälle tehdään AD:n käyttäjätilin ominaisuuksien määrittelyssä ADUC-työkalulla. Kuvassa 28 esitetään kotikansion linkitys.

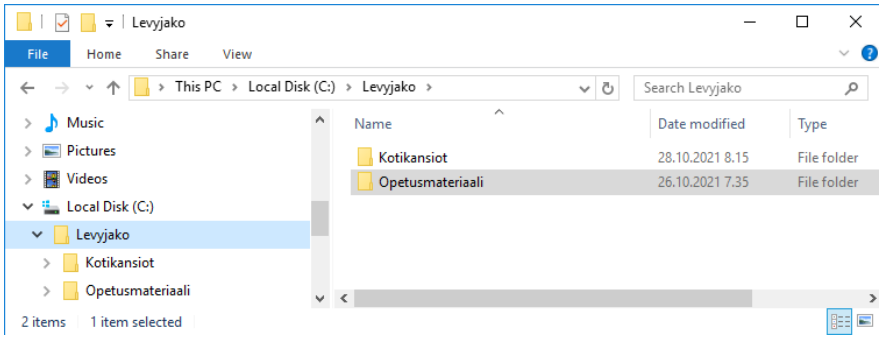


Kuva 28. Kotikansion (Home Folder) kansiopolku

Koulutusmateriaalin jakokansion eli M-aseman linkittäminen voidaan tehdä usealla eri tavalla. **Seuraavassa osiossa 4.4.3** esitetään eräs tapa. Kuitenkin aivan ensimmäinen vaihe on varsinaisten jakokansioiden luonti tallennusosiolle ja käyttöoikeuksien määrittäminen.

Tässä tapauksessa on käytettävissä ainoastaan yksi fyysinen palvelin ja siinä yksi vikasietoinen massamuisti. Käyttäjien jakokansiot tulevat olemaan aluksi samassa levyasemassa kuin varsinainen käyttöjärjestelmä. Tämän tyyppistä ratkaisua ei suositella, mutta tässä oppimis- ja koulutustarkoitukseen rakennettavassa ympäristössä voidaan toimia hiukan kompromisseja tehden. Voimme FSRM:n avulla helposti myös rajoittaa käyttäjien kotikansioiden kokoa, jolloin palvelimen kovalevyn täyttyminen ei tule yllätyksenä.

Seuraavassa oletettu jakokansio palvelimelle luotiin C:-aseman juureen resurssienhallinnalla. Jakokansion alle rakennettiin haluttu kansiorakenne, jossa esim. kotikansiot ja opetusmateriaalit jaetaan (kuva 29).



Kuva 29. Käyttäjille luotu jakokansio palvelimella

Kansioiden ja tiedostojen jako ja käyttöoikeuksien määrittely tehtiin halutun kansion kohdalla klikkaamalla hiiren oikealla painikkeella ja aukeavasta valikosta edettiin siten, että nimettiin *jako (share)* sopivan nimiseksi ja asetettiin halutut käyttöoikeudet kansioihin. Käyttöoikeudet asetettiin *Share (jako)- ja Security (suojaus)-puolelle*.

Käyttöoikeuksien määrittelyyn käytettiin perinteistä tapaa siten, että ensin asetettiin *Share-puolella Domain users*-käyttäjälle luku- ja kirjoitusoikeudet (Change) haluttuun kansioon. Sen jälkeen *Security-puolella (NTFS-oikeudet)* tehtiin varsinaiset tarkemmat ja tiukemmat käyttöoikeuksien määritykset jakokansioihin. Käyttöoikeudet määräytyvät aina lopulta alimman käyttöoikeuden mukaisesti. Share-oikeudet määrittävät käyttöoikeudet verkon kautta jakamiseen ja siinä on ainoastaan kolme käyttöoikeustasoa (full, change ja read). Security-puolella voidaan määritellä käyttöoikeudet hyvinkin tarkasti, joten sitä suositellaan käytettäväksi käyttöoikeuksien määrittämiseen varsinaisesti. [36, s.1029]

Käyttöoikeuksien määrittelyissä tulee olla huolellinen ja varovainen. *Käyttöoikeudet käyttäjille tulee aina asettaa ryhmien kautta*, ei yksittäisiä käyttöoikeuksia käyttäjille erikseen. Helposti myös saattaa unohtua esim. käyttöoikeuksien periytyminen yläpuoliselta kansiolta alikansioihin. Käyttöoikeuksien periytyminen alikansioihin voidaan tarvittaessa katkaista. Periytymisen katkaiseminen tapahtuu *Advanced*-painikkeen kautta ja sen tarjoaman näkymän kautta voidaan käyttöoikeuksia rajata huomattavasti tarkemmin. Mikäli ylläpitäjä on epävarma käyttöoikeuksien määrittelyssä, tulee ne aina testata varmuuden vuoksi eri testitunnuksilla. Tämän lisäksi suositellaan tutustumista parhaisiin käytäntöihin tiedostojen jaossa.

Tässä työssä annettiin käyttäjille luku- ja kirjoitusoikeudet omiin kotikansioihinsa verkossa, mutta opetusmateriaalin jakokansioon annettiin käyttäjille vain lukuoikeudet, jotta ne pysyisivät muuttumattomina. Peruskäyttäjille ei tulisi koskaan antaa täysiä oikeuksia mihinkään kansioihin vaan korkeintaan luku- ja kirjoitusoikeudet tilanteen mukaisesti.

4.4.3 Koulutusmateriaalin jakaminen verkkokansion avulla

Käyttäjän kirjautuessa omalla tunnuksellaan toimialueeseen, voidaan suorittaa eri asioita kirjautumisen yhteydessä esim. Logon-skripteillä. Skriptit voivat olla komentojonotiedostoja, VBS-skriptejä tai PowerShell-skriptejä. Isoissa organisaatiossa tulee huomioida kirjautumisprosessien nopeus, joten käytäntöjen

käyttöönotto tulee suunnitella ja testata huolellisesti. Verkonnopeus voi tulla myös pullonkaulaksi, mikäli käyttäjien lukumäärät ja yhtäaikaiset kirjautumisien määrät ovat suuria.

Verkkokansion jakaminen käyttäjille toimialueella voidaan tehdä useilla eri tavoilla. Jakokansion tulee olla luotuna ja valmisteltuna sekä jaettuna palvelimella. Perinteinen tapa on linkittää haluttu kansio käyttäjälle sisäänkirjautumisen yhteydessä. Tätä varten pitää tehdä ns. ”logon–skripti”, joka sitten suoritetaan käyttäjän sisäänkirjautumisen yhteydessä.

Tässä työssä käytetään *komentojonotiedostoa*, joka sisältää tarvittavat komennot kansion jakamista varten. Tämän jälkeen tiedosto (Login.bat) tallennettiin määrättyyn sijaintiin toimialueen ohjauskoneella. Lopuksi lisättiin ADUC-työkalulla käyttäjän profiiliasetuksiin Logon script:-kenttään ajettavan komentojonotiedoston nimi (Login.bat). Seuraavassa esitetään työvaiheet:

- Tehdään **Login.bat** tiedosto (esim. Notepad-teksturilla), joka sisältää halutut komennot esimerkiksi:

  ```
  Net Use M: \\ServerName\ShareName
  ```

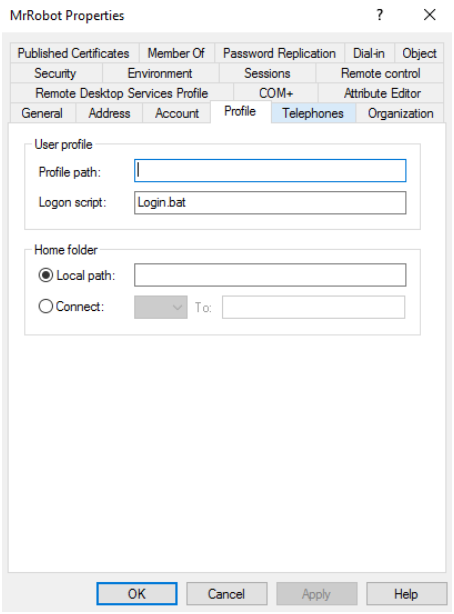
- Tallennetaan tämä tiedosto DC:lle määrättyyn kansioon eli sijaintiin:

  ```
  C:\Windows\SYSvol\sysvol\[domain].local\scripts
  ```

- Lisätään ko. käyttäjän profiiliasetuksiin kenttään Logon script: **Login.bat**

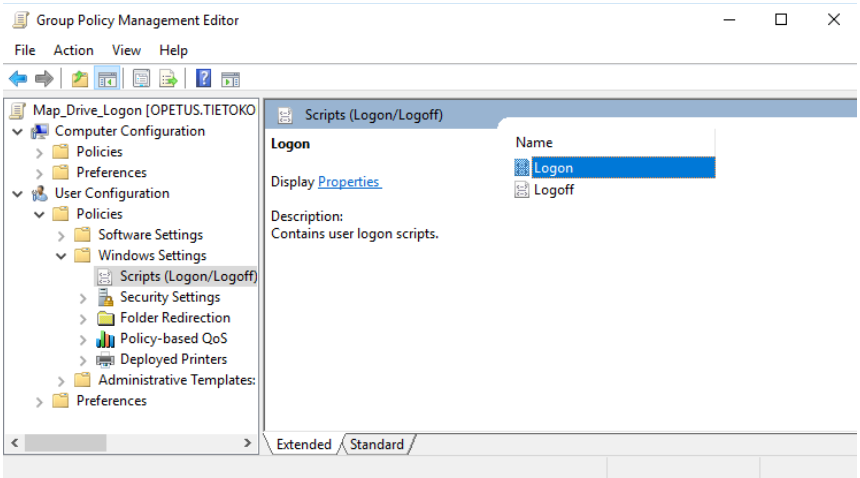
- Testataan toiminta varmuuden vuoksi testitunnuksella.

Kuvassa 30 esitetään käyttäjän profiiliasetuksiin lisätty Logon script (komentojonotiedosto:**Login.bat**).



Kuva 30. Logon scriptin lisääminen

Toinen tapa on tehdä halutun jakokansion linkitys siihen tarkoitukseen tehdyn *ryhmäkäytännön avulla* lisäämällä Logon-skripti ryhmäkäytäntöön kuvassa 31 esitettyyn positioon eli sijaintiin ohjainkoneella. Määrittelyssä tehdään komentojonotiedoston valmistelu ja tallennus samalla tavalla kuin edellisessä kohdassa, mutta komentojonotiedosto lisätään ryhmäkäytännön osoittamaan paikkaan, kuten **liitteessä 2** on esitetty. [37]



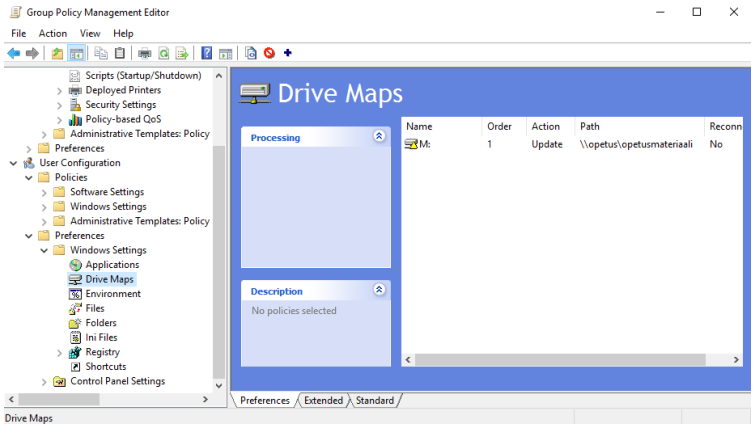
Kuva 31. Ryhmäkäytäntö Map_Drive_Logon

4.4.4 AD:n Preferences-laajennuksen käyttö (Drive Maps)

Tässä työssä käytettiin tällä kertaa halutun kansion jakoon käyttäjille hyödyntäen Active Directoryyn myöhemmin (Windows Server 2008 jälkeen) käyttöön otettua Group Policy Preferences -laajennusta. Se tarjoaa monipuolisemman tavan määritellä työaseman asetuksia ja sovelluksia. Sillä voi korvata esim. Logon-skripteillä aikaisemmin tehtäviä toimintoja. AD:n Preferences eivät ole varsinaisia ryhmäkäytäntöasetuksia, vaan ne ovat periaatteessa käyttäjäpuolen laajennuksia. [38]

Tällä tavalla tehty asetuksien määrittely jää pysyväksi tietokoneen rekisteriin käyttäjälle, vaikka linkitys poistettaisiin myöhemmin. Se tekee työaseman rekisteriin samaan haaraan ja paikkaan muutokset kuin työasemapuolella paikallisesti tallennetaan. Tämän lisäksi käyttäjän on mahdollista muuttaa asetuksia jälkeenpäin myöhemmin, eikä asetusta voida näin ollen pakottaa niin kuin ryhmäkäytännöillä tehdään. Näihin Preferences-hallintamahdollisuuksiin kannattaa perehtyä huolellisesti, mikäli niitä alkaa hyödyntämään laajemmin.

Seuraavassa kuvassa 32 esitetään miten esim. levyn ”mäppäys” on määritettynä. Tämän työn yhteydessä emme käy tätä menetelmää yksityiskohtaisesti lävitse, mutta käyttöympäristön jatkokehityksessä menetelmän hyödyntäminen saattaa tulla kysymykseen. Tämän tyyppistä määrittelytapaa voidaan käyttää tarvittaessa, mutta se ei korvaa perinteistä ryhmäkäytännöillä tehtäviä määrittelyjä.



Kuva 32. Drive Maps (Preferences)

5 Palvelimien tietoturva, etähallinta ja varmistukset

Palvelimien tietoturvaan tulee kiinnittää erityistä huomiota, koska niiden on tarkoitus toimia luotettavasti ja tietoturvallisesti. Palvelimien tulee tarjota verkkopalveluita usein laajalle asiakaskunnalle ympäri vuorokauden ja asiakkaiden tietosuojan tulee olla myös lain mukaan riittävän korkealla tasolla. Ulkopuoliset eivät saa päästä käsiksi luottamuksellisiin tietoihin paikallisesti eikä verkon kautta.

Palvelimiin kohdistuu runsaasti hyökkäyksiä verkon kautta, joten verkkorajapinnat tulee olla kunnossa ja kaikki verkon aktiivilaitteet päivitettynä 24/7. Tietoturvaan kannattaa kiinnittää jo palvelininfrastruktuurin suunnitteluvaiheessa, tällöin voidaan myös asennuksissa noudattaa parhaita ja turvallisia käytäntöjä. Lisäksi kriittisissä järjestelmissä tulee käyttöjärjestelmät mahdollisesti ”kovettaa”, jolloin oletusarvoja asennuksissa ei tällöin voitaisi käyttää. Tämä asettaa melkoisen lisähaasteen pääkäyttäjille.

Nykyisin laissa määritellään pitkälti säännöt ja standardit mitä tulisi noudattaa palvelininfrastruktuurin rakentamisessa. Tietoturvallisuuden suunnittelu lähtee riskien arvioinnista ja hallinnasta. Riskienarvioinnin pohjalta tulisi rakentaa riittävän turvallinen toimintaympäristö. Tietoturvallisuus tulee optimoida palvelun kriittisyyden mukaan ja se vaatii ymmärrystä ja riittäviä resursseja. Järjestelmien rakentamisessa kannattaa käyttää tarvittaessa asiantuntijayrityksiä. Seuraavassa osiossa käydään läpi muutamia tärkeitä seikkoja liittyen palvelimien tietoturvaan.

Tietoturva ei kuitenkaan yksin riitä, vaan yhä enenemässä määrin tulee myös kiinnittää huomioita esim. *ympäristöarvoihin ja hiilijalanjäljen minimoimiseen*. (Kappaleessa 6 sivulla 76 lisätietoja kestävästä kehityksestä ICT-tuotannossa).

5.1 Palvelinympäristö

Ympäristöolosuhteet palvelimille tulee tehdä suotuisiksi ja turvallisiksi. Maapallolla ympäristöolosuhteet vaihtelevat, joten suojaukset Suomessa ovat erilaiset kuin jossain epävakaammilla alueilla, joissa tulee varautua esim.

hirmumyrskyihin, tulviin tai maanjäristyksiin. Usein suuret palvelinkeskukset rakennetaan juuri sen mukaan niille seuduille, missä on rauhallisemmat olosuhteet. Tänä päivänä palvelinkeskuksien rakentamisessa huomioidaan myös kestävän kehitykseen liittyvät seikat, kuten hukkalämmön talteenotto tai viileän ilmaston läheisyyden hyödyntäminen jäähdytyksessä. Palvelinkeskuksen sijainti tulee sijaita myös poliittisesti vakaalla maaperällä ja energian (vihreä) saanti pitää olla varmistettu.

Fyysinen tila ja valvonta

Palvelintilassa ei saa olla lainkaan ikkunaa ja oven vahvuus pitää olla normaalia tukevampi. Asiattomat eivät saa päästä fyysisesti käsiksi palvelimeen, joten lukitus ja murtosuojaus pitää olla kunnossa. Tilassa tulisi tarvittaessa olla sähköinen kulunvalvonta ja mahdollisesti kameravalvonta sekä murtohälytinjärjestelmä. Palvelimien sijoitteluun palvelintilassa tulee kiinnittää huomiota ja sijoittelu esim. palvelinräkkiin, joka on lukittu, lienee tehokas ratkaisu myös jäähdytyksen ja tilan käytön kannalta. Palvelimissa tulee käyttää myös paikallista salausjärjestelmää, kuten esim. Microsoftin tarjoamaa **BitLocker**-tiedonsuojausjärjestelmää. [39]

Ideaalitilanteessa palvelintila ympäristöineen on hallittu ja valvottu monin tavoin. Palvelintilan tulee olla rakennettu palvelutason kriittisyysasteen mukaisesti. *Paloturvallisuuden* tulee olla hyvin korkealla tasolla. Mitään turhaa palokuormaa ei saa olla tilassa. *Tilassa käytettävät sammuttimet tulee olla oikeanlaiset (CO_2)* ja palohälyttimet kunnossa. Tämän lisäksi automaattiset tulipalon sammutusjärjestelmät tulisivat olla myös oikeanlaiset. [39]

Vesivahinkoihin on varauduttava siten, että laitteet ovat riittävällä korkeudella lattian pinnasta ja vesijohtoja ei saa kulkea tilan päällä. Ympäristöolosuhteiden muutoksista palvelintilassa tulee lähteä tarvittaessa hälytys automaattisesti päivystykseen, jotta voidaan ryhtyä toimenpiteisiin mahdollisimman nopeasti. [39]

Lämpötila ja jäähdytys

Lämpötilan hallinta ja jäähdytys tulee järjestää. Pienissä järjestelmissä ja tiloissa saattaa riittää laitetuulettimet, mutta silloin tilan peruslämpötila ei myöskään saa-esim. kesäisin nousta liian korkealle. Palvelintilan suositeltu lämpötila-alue lienee 22-27 °C ja ilmankosteus 40–60 % rajoissa. Toisaalta nykysuuntaus laitehuoneen lämpötilasuosituksissa on energiansäästön kannalta nousemaan päin. Nykyisin saattaa jopa 27 °C olla riittävän alhainen lämpötila palvelintilaan. Jäähdytysjärjestelmissä tulee ottaa huomioon myös ympäristöarvot. Hukkalämmön talteenotto ja luontaisen ympäristön hyödyntäminen jäähdytyksessä ovat erittäin tärkeitä huomioitavia seikkoja nykyisin. [39]

Sähkönsyöttö

Sähkö lienee kaiken nyky-yhteiskunnan perusta ja ilman sitä olemme käytännössä keskiaikaisessa toimintaympäristössä, joten kaikki kunnia sähkön keksijöille. Sähkönsyöttö palvelimille tulee varmistaa ja suodattaa UPS:n (Uninterruptible Power Supply) avulla. UPS-järjestelmät suojaavat laitteita mm. lyhyiltä sähkökatkoilta ja sähköpiikeiltä. Palvelimet tulee ajaa tarvittaessa automaattisesti tai manuaalisesti hallitusti alas, mikäli sähkökatko kestää yli akuston sähkövarannon. Kriittisissä yhteiskunnallisissa toiminnoissa, kuten sairaaloissa tarvitaan lisäksi esim. *varageneraattorit ja polttoainevarastot*, jotta voidaan varautua pidempiin sähkökatkoksiin. [39]

Verkko ja verkkolaitteet

Verkkoyhteyksien ja tietoliikenneverkkojen merkitystä ei voi liikaa korostaa. Ilman tietoliikenneverkkoa ei ole palveluita, eikä mitään muutakaan, joten ne ovat tänä päivänä lähes yhtä tärkeitä kuin sähköverkot. Tietoliikenneyhteydet tulee olla mielellään kahdennettuja ja niiden kapasiteetti tulee olla riittävä, myös käyttöpiikkien aikana. Tällöin esim. eri virtualisointitekniikat lienevät parhaimpia vaihtoehtoja myös verkkopuolella, koska ne skaalautuvat tarvittaessa automaattisesti käytön mukaan. Oma lähiverkko pitää olla rakennettu asiallisesti tietoturva

huomioiden. Lähiverkko tulee olla segmentoitu virtuaalisiin aliverkkoihin ja rajapinnoissa tulee käyttää palomuureja ja verkon valvontalaitteita. [39]

Kyberturvallisuuteen tulee kiinnittää erityistä huomiota ja verkkolaitteiden tietoturvallisuus ja luotettavuus tulee olla korkealla tasolla. Erittäin tärkeätä on huomioida se, että verkkolaitteiden konfiguroinnit on tehty oikeaoppisesti ja päivitykset niissä ovat ajantasaisia. Tämän lisäksi tulee käyttää verkon tietoturvaa lisääviä laitteita ja tekniikoita sekä valvontajärjestelmiä. Sanomattakin on selvää, että salausjärjestelmiä tulee käyttää nykyään lähes kaikessa tiedonsiirrossa ja tietojen varastoinnissa. *Langattomat verkot* ovat sitten oma lukunsa ja niiden merkitys korostuu etenkin asiakasrajapinnassa. Langattomissa verkoissa tulee käyttää uusimpia ja turvallisimpia salaustekniikoita.

Oman palvelintilan rakennus- ja ylläpitokustannukset sekä energiankulutus ovat melko suuria. Tällöin palveluiden ulkoistaminen saattaisi olla kelpo ratkaisu ainakin osittain. Pienissä yrityksissä saatetaan tehdä vielä kuitenkin kompromisseja omien tilojen kohdalla, koska yritystoiminnan kriittisyysaste vaihtelee riippuen organisaation toimialasta ja koosta. Palvelininfran suunnittelussa ja rakentamisessa tulee käyttää ehdottomasti asiantuntijapalveluita. [39]

5.2 Palvelimen vikasietoisuus

Palvelimen vikasietoisuutta voidaan parantaa monin tavoin. Palvelimissa on usein hallinta- ja valvontaohjelmistoja, joilla voidaan seurata palvelimen tilaa. Samoin niissä on usein erillinen etähallintaliitäntä, jonka kautta voi tietoturvallisesti hallita palvelinta, vaikka se olisi sammutettuna. Luonnollisesti virtualisointitekniikat tarjoavat huomattavasti paremman ja helpomman ratkaisun vikasietoisuuden kasvattamiseen kuin perinteiset tekniikat.

Hankittaessa omaa palvelinrautaa kannattaa suosia tunnettuja valmistajia sekä käyttää energiatehokkaita, laadukkaita, kestäviä ja testattuja komponentteja. Usein vikaantuvat komponentit ja moduulit voidaan kahdentaa, kuten tässä työssä käytetyssä palvelimessa on kahdennettu virtalähde ja verkkokortti sekä

kovalevyt. Virtalähteet ja kovalevyt ovat usein Hot Plug-tyyppisiä, jolloin niiden kytkeminen onnistuu palvelimen olleessa käynnissä, eikä ne vaadi palvelimen uudelleen käynnistystä. Palvelimien massamuistien vikasietoisuuttaa voidaan lisätä mm. Redundant Array of Independent Disks (RAID) -levyjärjestelmillä.

RAID-levyjärjestelmät

RAID (Redundant Array of Independent Disks) -levyjärjestelmäratkaisuja on käytetty palvelimissa ja tehotyöasemissa jo vuosikymmeniä vikasietoisuuden kasvattamiseksi. On kuitenkin huomioitava, että ne eivät korvaa säännöllistä ja huolellisesti toteutettua varmuuskopiointisuunnitelmaa. [40]

RAID 0

RAID 0 (lomitus) ei lisää vikasietoisuutta, mutta levyn luku- ja kirjoitusnopeus kasvaa. Tätä ei kannata käyttää kriittisissä järjestelmissä. [40]

RAID 1

RAID 1 eli peilaus kahden levyn tapauksessa kirjoittaa molemmille levyille saman datan, jolloin toisen levyn vikaantuessa, tiedot ovat palautettavissa toisesta levystä. Lukunopeus parhaimmillaan periaatteessa kaksinkertaistuu. [40]

RAID 5

RAID 5:n muodostamiseen tarvitaan vähintään kolme levyä. RAID 5 -järjestelmä hajauttaa tiedot kolmelle levylle siten, että sietää yhden levyn rikkoontumisen. Tiedot ovat palautettavissa pariteettitietojen avulla, kun ehjä levy lisätään takaisin pakkaan. Luku- ja kirjoitusnopeus kasvaa verrattuna yhteen levyyn. [40]

Tämän lisäksi on olemassa muita RAID-järjestelmiä, jotka ovat edellisten kombinaatioita esim. RAID 10, jossa on huomioitu nopeus ja vikasietoisuus. [40]

Tässä työssä käytetyssä palvelimessa valittiin laitepohjaiseksi levyjärjestelmäksi RAID 1 -levyjärjestelmä. RAID 1 -levyjärjestelmän muodostamiseen tarvittiin kaksi saman kokoista SSD-levyä (2 X 960 GB), jotka hankittiin palvelimen asennuksen yhteydessä. RAID 1 -levyjärjestelmä peilaa tiedot toiselle levylle, jolloin yhden levyn rikkoontuessa tiedot ovat vielä tallessa toisessa levyssä. Periaatteessa myös lukunopeus saattaa tuplaantua ainakin ideaalitilanteessa.

5.3 Palvelimien etähallinta

Nykyisin palvelimien hallinta tapahtuu pääsääntöisesti etähallintana verkon kautta. Palvelimiin saa yleensä erillisen liitännän avulla etäyhteyden, vaikka palvelin olisi sammuksissa. Tässä työssä käytetyssä Dellin palvelimessa on Integrated Dell Remote Access Card 7 (iDRAC7) -ohjain, jonka kautta voidaan etähallita palvelinta. Laite sijaitsee palvelimen emolevyllä ja sen avulla ylläpitäjät voivat suorittaa etähallintatehtäviä. [41]

Tässä perinteisessä Dellin palvelimessa pyörii *Open Manage Server Administrator (OMSA)* -järjestelmänhallintaratkaisu yhdelle palvelimelle. Sen avulla voidaan hallita palvelinta käyttöjärjestelmän komentoriviliittymässä tai graafisessa selainpohjaisessa liittymässä. Dell tarjoaa myös *Open Manage Enterprise (OME)* -järjestelmäratkaisun koko infrastruktuurin hallintaan. [41]

Pilvipalveluiden etähallintaratkaisut (Azure)

Kaikissa nykyisissä pilvipalveluissa, kuten Microsoftin Azuren pilvipalveluissa, joissa esim. virtuaalipalvelimet sijaitsevat on käytössä omat tietoturvalliset etähallintaratkaisut. Pilvipalveluita hallitaan verkon yli tietoturvallisesti usein graafisilla käyttöliittymillä, kuten web-selaimella (https://) esim. Azuren portaalissa. Tämän lisäksi Azuren hallintaan voi käyttää monia eri tapoja: [42]

- PowerShell (komentorivitulkki)
- Azure CLI (komentorivitulkki)
- Azure Management Libraries for .NET

- Azure Java API, Azure SDK, Azure Python libraries, etc.
- Azure REST API
- ARM Templates (JSON).

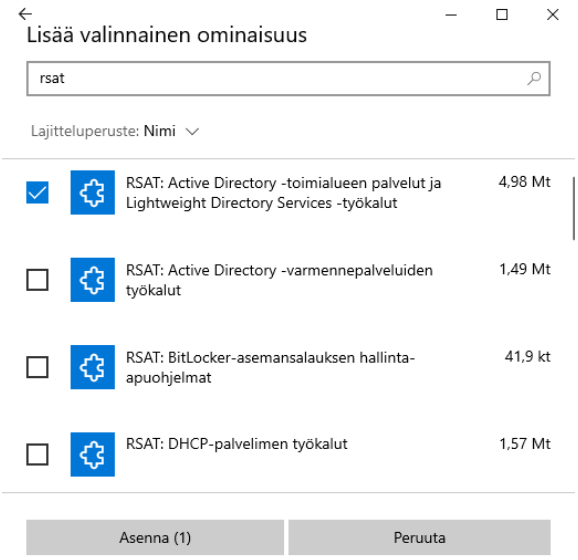
Remote Desktop Connection

Yksinkertaisimmillaan etäyhteys voidaan järjestää Windows-palvelimeen käyttöjärjestelmän tarjoamalla Remote Desktop Connection -apuohjelman avulla. Etäyhteysohjelma on graafinen ja perustuu Microsoftin Remote Desktop Protocol -yhteysprotokollaan (RDP). Toisaalta tässä ratkaisussa voidaan hallita palvelinta ainoastaan silloin, kun se on linjoilla ja elossa. Tämän tyyppisessä ratkaisussa tulee huomioida se, että etäyhteys on riittävän tietoturvallisesti (salattu) järjestetty. Etäyhteys sallitaan palomuurissa palvelimen käyttöjärjestelmässä. Palvelimen palomuuriin on suositeltavaa määritellä mm. pääsylistat etähallintaa varten ja tarvittaessa rajoittaa hallinta vain rajatulle joukolle ylläpitäjiä. RDP-yhteyttä palvelimeen ei tule sallia Internet-rajapinnasta, ellei sitä voida tietoturvallisesti tehdä. [43]

5.4 Windows palvelimien etähallintatyökalut (RSAT)

Microsoftin Windows työasemiin voidaan asentaa palvelimien etähallintaan tarkoitetun RSAT (Remote Server Administration Tools) –työkalupaketin. Se on Microsoftin kehittämä työkalu, joka esiteltiin jo Windows Server 2008 R2 yhteydessä. RSAT-työkalulla voidaan etähallita Windows-palvelimia.

RSAT-työkalu sisältää hallintatyökalujen lisäksi mm. MMC-laajennukset, komentorivityökalut ja PowerShellin -cmdletit. Kuitenkin on huomioitava se, että kyseisellä pääkäyttäjällä tulee tietenkin olla käyttöoikeudet hallittaville palvelimille. Nykyisin (11/2018 jälkeen) sen voi asentaa esim. Windows 10 Professional ja Enterprise versioihin suoraan käyttöjärjestelmän lisäominaisuuksien kautta. Lisäominaisuuden voi suoraan lisätä työasemaan, kuten kuvassa 33 esitetään. [44]



Kuva 33. RSAT-työkalun lisääminen työasemaan

Toinen vaihtoehto on ladata RSAT-työkalupaketti Microsoftin internet-sivustolta. [44]

5.5 Palvelimen terveystarkistus

Palvelin tulee ns. ”terveystarkistaa” ennen virallista käyttöönottoa. Siinä voi käyttää apuna erilaisia siihen tarkoitettuja tarkistusohjelmia. Käyttöjärjestelmän mukana tulevalla *Best Practices Analyzer* -työkaluohjelmalla tehty tarkistus saattaa löytää jotain korjattavaa tai huomautettavaa. Palvelimen Best Practices Analyzer löytyy Server Managerista. Palvelimen tapahtumalokit on syytä myös käydä lävitse mahdollisten virheilmoituksien varalta. [45]

Tapahtumalokien seuranta kuuluu niin ikään normaaliin ja säännöllisiin toimiin ylläpitäjillä, joten niitä ei sovi unohtaa ja tarvittaessa hälytykset voikin automaattisesti lähettää päivystäjälle esim. sähköpostilla. AD-palvelimelle löytyy myös erinomaisia työkaluohjelmia palvelimen toiminnan tarkistamiseen. Komentorivipohjaisista työkaluohjelmista perinteisten verkkokomentojen lisäksi mainittakoon Active Directoryn komentokehotteessa toimivat perustyökalut: **Adprep** ja **Dcdiag**.

Windows Update -päivityksien tarkistus ja niiden asennus tulee tehdä säännöllisesti ja heti kun ne ovat saatavilla. Päivitykset tulee yleensä automatisoida, mikäli mahdollista. Kaikki tarpeettomat palvelut kannattaa poistaa palvelimesta, mikäli niitä ei tarvita. Palomuurin asetukset on syytä tarkistaa ja poistaa tarpeettomat sallimukset palomuurista sekä sisään tulevalle, että ulospäin lähtevälle verkkoliikenteelle. Palvelimessa tulee käyttää myös jotain laadukasta ja hyvin integroitua virussuojausohjelmaa, kuten esim. käyttöjärjestelmän mukana tuleva Microsoftin oma Windows Defender -suojausohjelmaa. Palvelimelle on suositeltavaa myös aika ajoin suorittaa täydellinen virustarkistus. Palvelinta ei tule käyttää missään tapauksessa internet-selailuun ja hakuihin internetissä.

Verkkoskannaus esim. samasta aliverkosta tarkistettavaan palvelimeen päin on eräs tapa varmistaa, että tarpeettomia palveluita eli portteja ei ole palvelimessa auki ulkomaailmaan. Verkkoskannaus voidaan tehdä esim. Zenmap-ohjelmalla verkosta käsin samassa aliverkossa olevalta työasemalta. Verkkoskannausta varten tarvitaan aina verkon omistajan lupa, jotta vältytään väärinkäsityksiltä ja virhehälytyksiltä. [46]

5.6 Varmistukset

Tiedot ovat organisaatioiden tärkeimpiä resursseja ja varantoja työntekijöiden lisäksi. Tietojen suojaamiseksi ja varmistamiseksi tulee tehdä mahdollisemman hyvät suunnitelmat ja se kuuluukin tietoturvallisuuden normaalin ylläpitokonseptiin. Palvelimien vikasietoisuuden optimointi on tärkeää, mutta sen lisäksi on otettava varmistuksia järjestelmistä ja tiedoista. Palvelimista tulee ottaa varmistuksia säännöllisesti ja riittävän usein riippuen palvelun ja tietojen kriittisyydestä.

Varmistukset tulee automatisoida, koska omaan muistiin luottaminen ei ole vaihtoehto. Järjestelmien ja tietojen palauttamisprosessit tulee olla kohtuullisen nopea, jotta organisaation toiminta voidaan palauttaa ennalleen katastrofin jälkeen mahdollisimman nopealla aikataululla. Huomioitavaa on myös se, että palautuksia kannattaa aika ajoin testata, jotta saadaan selvyys niiden toimivuudesta.

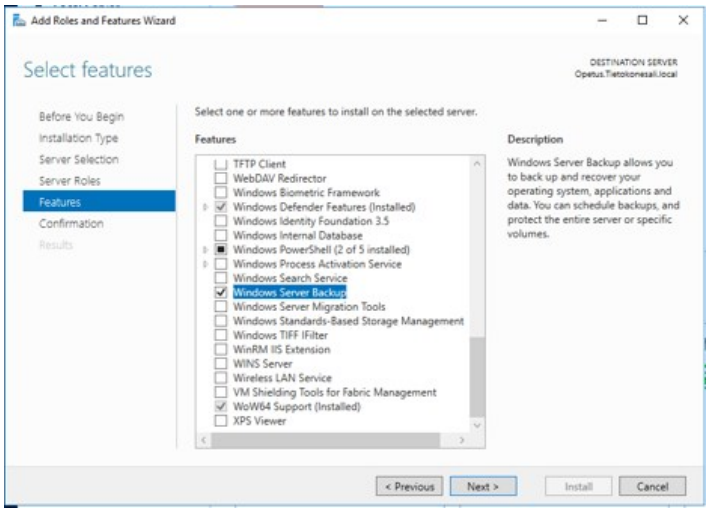
Virtualisoiduista palvelimista on huomattavasti kätevämpi ottaa varmistuksia ja levykuvia palvelun kriittisyyden ja tarpeen mukaan. Samaten palautukset sujuvat nopeasti ja joustavasti tarvittaessa. Perinteisessä ympäristössä varmistukset ja palautukset ovat hiukan haasteellisempia. Aikoinaan käytettiin myös varmistusnauhoja ja nauharobotteja. Nauhojen käyttö varmistuksiin oli hidasta ja kallista. Nauhat ja nauha-asemat olivat myös erittäin vikaherkkiä, joten ne lienevät katoavaa varmistustekniikkaa lähitulevaisuudessa.

Active Directory on yleisesti ottaen kriittisimpiä verkkopalveluita organisaation sisäverkossa. AD:n vikaantuessa vaikutukset voivat olla hyvin laajoja, jopa koko organisaation laajuisia. Lähtökohtaisesti toimialueessa tulisi olla vähintään kaksi ohjainkonetta eli Domain Controlleria, jotta yhden vikaantuessa toinen vielä tarjoaa palveluita. Varmistuksia tulisi ottaa kaikista toimialueen ohjainkoneista erikseen. Varmistukset tulisi säilöä turvallisesti ja vähintään kahdessa eri fyysisessä sijainnissa.

Varmistuksia palvelimesta voidaan ottaa osittaisina tai täysinä varmistuksina. Varmistuksia voidaan ottaa myös pelkästään esim. datakansioista tiedon kriittisyyden mukaan. Varmistuksien ottoon voidaan käyttää käyttöjärjestelmän tarjoamia varmistusohjelmia tai erillisiä siihen käyttötarkoitukseen tehtyjä varmistusohjelmia muilta ohjelmistotoimittajilta.

5.6.1 AD-palvelimen täysi varmistus

AD-palvelimen täydessä varmistuksessa otetaan koko järjestelmän data kansioineen talteen ja ne voidaan palauttaa kerralla takaisin palvelimeen. Tässä työssä käytetään Microsoftin palvelinohjelmiston mukana tulevaa **Windows Server Backup** -ohjelmaa. Tämä ohjelma eli ominaisuus (feature) pitää asentaa palvelimeen erikseen. Kaikki palvelimen mahdolliset lisäominaisuudet ovat asennettavissa **Server Managerin Dashboardista** keskitetysti kohdasta **2. Add roles and features. Valitaan Windows Server Backup** ja asennetaan ohjelma (kuva 34). [47]



Kuva 34. Windows Server Backup-ohjelman asennus

Asennuksen jälkeen Varmistusohjelma löytyy Server Managerin Tools-valikosta→ **Windows Server Backup**. **Liitteessä 3** esitetään esimerkkinä täysi varmistus palvelimesta.

5.6.2 AD-palvelimen palautus täydestä varmistuksesta

Järjestelmän palauttaminen täydestä AD-palvelimen varmistuksesta tehdään käynnistämällä palvelin Windows Server -asennuslevyltä tai vastaavasti USB-tikulta. Asennusohjelmiston käynnistymisen jälkeen edetään seuraavasti:

Repair your computer→ Troubleshoot→Advanced options→ System Image Recovery ja valitaan Windows Server 2016. Tämän jälkeen aukeaa ikkuna, josta valitaan viimeisin saatavilla oleva varmistus, josta palautus tehdään. AD:n palautus voidaan tehdä *määräävänä eli autoritäärisenä tai ei määräävänä eli ei-autoritäärisenä*. Tähän otetaan kantaa palautusohjelman valinnoissa. Tässä työssä on vain yksi Domain Controller, joten valinnalla ei ole tässä yhteydessä merkitystä, koska palvelin toimii kaikissa AD:n sisäisissä rooleissa ja on luonnostaan primääripalvelin. [47]

Autoritäärinen palautus

Autoritäärinen palautus tarkoittaa sitä, että palautettavaan palvelimeen ei replikoida muista Domain Controllereista mahdollisia muutoksia AD:n objekteista. Autoritäärinen palautus voidaan tehdä koko tietokannalle tai vaikkapa vain tietylle säiliölle kuten organisaatioyksiköllle ja sen alla oleville objekteille. Palautuksessa käytetään hyväkseen usein AD:n tietokannan hallintaan tarkoitettua komentokehotetyökalua: **Ntdsutil.exe**. [47]

Ei-autoritäärinen palautus

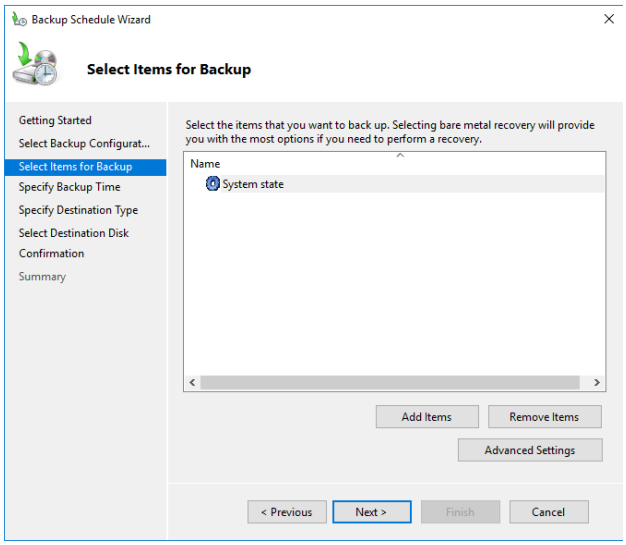
Tämä palautusmetodi on vastakohta edelliselle. Siinä palautuksen jälkeen replikoidaan palvelimen tietokantaan kaikki varmistuksen jälkeiset muutokset AD:n objekteista muilta toimialueen ohjauskoneilta. [47]

5.6.3 AD-palvelimen System state -varmistus

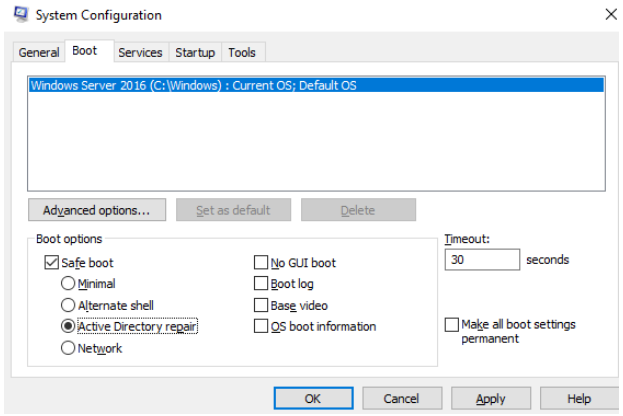
System state -varmistus (kuva 35) ottaa Active Directoryn (AD DS ja Ntds.dit) lisäksi palvelimelta talteen mm. rekisterin, käynnistys-, järjestelmätiedostot, Sysvol-kansion, COM+ luokan rekisteröintitiedot, DNS-tiedot ja levyn osiointitiedot. Tällöin järjestelmä voidaan palauttaa ilman uudelleen konfigurointia. Huomioitavaa on se, että tässä varmistustavassa ei oteta varmistusta palvelimeen asennetuista ohjelmista ja käyttäjien mahdollisista erillisistä datatiedostoista.

Järjestelmän palauttaminen tehdään palvelimen *vikasietotilassa* (kuva 36). Palvelin saadaan käynnistymään ns. vikasietotilaan suorittamalla komento: **msconfig** ja valitsemalla **Boot**-välilehdeltä valinta **Active Directory repair**. Käynnistyksessä kirjaudutaan **DSRM**-moodissa palvelimeen ja tehdään järjestelmän palautus. Kirjautuminen tapahtuu AD:n asennuksessa tehdyllä DSRM-palautussalasanalla. Huomioitavaa on myös se, että kirjaudutaan paikallisesti palvelimeen ei toimialueeseen. **System state** -varmistusta suositellaan yleensä tehtäväksi kaikkiin toimialueella oleviin Domain Controllereihin eli ohjainkoneisiin. Tämä antaa

suojaa mm. ylläpitäjän vahingossa tekemiin poistoihin tai muihin vastaaviin tiedon korruptoitumisiin AD:ssä. [47]



Kuva 35. System state varmistus AD-palvelimessa



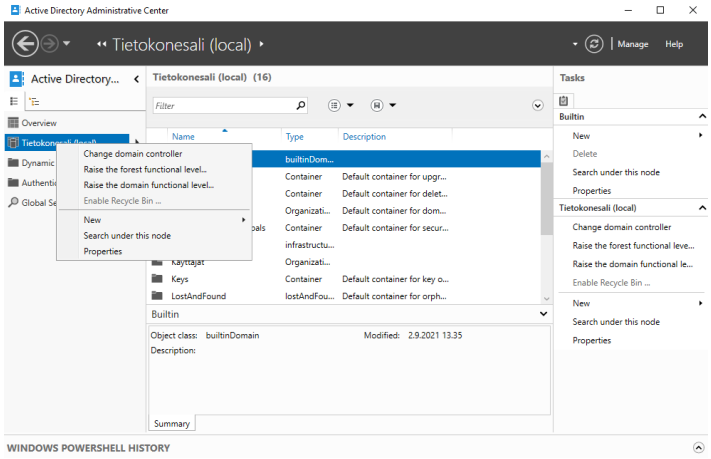
Kuva 36. AD-palvelimen käynnistäminen vikasietotilaan

5.6.4 Active Directory -palvelimen roskakorin käyttöönotto

AD-palvelimen roskakori on suositeltavaa ottaa käyttöön, koska AD:n hallinnassa voi vahingossa esim. poistaa objekteja. Tällöin roskakorista voi kätevästi ja nopeasti palauttaa poistetut objektit kaikkine parametreineen. Palautuksen voi

tehdä palvelimen ollessa tuotannossa, joten pitkiä katkoja palveluun ei synny, kuten esim. System state -palautuksessa. [47]

Palvelimen ”Roskakori-toiminto” voidaan ottaa käyttöön graafisella **Active Directory Administrative Center (ADAC)** -työkalulla. Valitaan haluttu palvelin aktiiviseksi ja hiiren oikealla painikkeella saadaan näkyviin pikavalikko, josta valitaan kohta **Enable Recycle Bin…**Kuvassa 37 näkyy käyttöönotettu Roskakori-toiminto.



Kuva 37. AD-palvelimen Roskakori otettu käyttöön

5.6.5 Varmistuksien ajastukset ja automatisoinnit

Varmistuksien ottaminen voidaan automatisoida ja ajastaa sopivasti esim. yö- tai ilta-aikaan tehtäviksi, jolloin ne eivät häiritse tuotantoa. Toisaalta jotkut palvelimet ovat käytännössä koko ajan tuotannossa ja tarjoavat palveluita 24/7, joten varmistusstrategia on luotava tuotannon edellyttämällä tavalla. Varmistustapoja ja suosituksia on monenlaisia riippuen ympäristöstä ja palvelujen kriittisyydestä. Varmistussykli voi olla esim. kerran vuorokaudessa tai kaksi kertaa vuorokaudessa riippuen tietojen kriittisyydestä. Voidaan käyttää myös tehokkaampaa tapaa siten, että tehdään täysivarmistus kerran kahdessa viikossa ja sitten 14 kpl:tta ns. differentiaalista varmistusta, joka ottaa vain muuttuneet tiedot talteen. Varmistuksien ottaminen on silloin nopeampaa, mutta palautuksissa vastaavasti

saattaa kulua enemmän aikaa riippuen valitusta menetelmästä. Palvelutuotannon aikakriittisyys on syytä huomioida varmistusstrategiaa luodessa.

Varmistukset tulee salata riittävällä salausalgoritmilla ja varmistuksien säilytyspaikkoja tulisi olla vähintään kaksi toisistaan riippumatonta fyysistä sijaintia esim. paikallinen tallennus palvelintilassa ja toinen esim. salatussa pilvessä (omassa tai ulkoisessa) tai fyysisesti kassakaapissa. Mikäli pilvipalveluita käytetään, tulee niiden tietoturvallisuudesta varmistua erilaisin käytännöin ja sopimuksin.

6 Ympäristöarvot ja energiankulutus

Ympäristöarvojen huomioiminen kaikissa toiminnoissa nykyisessä yhteiskunnassa on erittäin tärkeää ja ainut elinehto elämän jatkuvuudelle planeetallamme. Kestävän kehityksen periaatteet tulisi ohjata ihmisen toimintaa kaikilla elämän osa-alueilla, kuten myös tieto- ja viestintätekniikassa. Tänä päivänä pahimmat maailmanlaajuiset riskit, kuten ilmastonmuutos ja siihen liittyvä luonnon monimuotoisuuden katoaminen on nykyihmiskunnan ansiosta realisoitumassa lähitulevaisuudessa. Tästä johtuen kaikkien ihmisten ja organisaatioiden tulisi panostaa kaikki liikenevät resurssit ns. vihreään siirtymään ja sen nopeuttamiseen.

Maailma sähköistyy ja tietotekninen infrastruktuuri toimii sähköllä, jolloin nykymuotoisen yhteiskunnan tärkeät perustoiminnat ovat toimivan ja vastuullisen energiantuotannon varassa. ICT-teknologia tarjoaa paljon hyviä ratkaisuja ilmastomuutoksen hillitsemiseksi, mutta tietotekninen infrastruktuuri itsessään aiheuttaa jo kohtalaisen paljon päästöjä. Energiatuotanto tulee järjestää hiilineutraalisti ja ympäristöarvoja kunnioittaen. Sähkönkulutuksen vähentäminen on eräs tapa vähentää päästöjä ja se on myös kustannuspoliittisesti järkevää toimintaa.

Laitteiden alhainen sähkönkulutus tai ns. *energiatehokkuus* ja kehittyneet virransäästöominaisuudet tulee olla laitteiden hankintakriteerien kärkipäässä. Kannettavat tietokoneet kuluttavat sähköä murto-osan pöytätyöasemiin verrattuna, mutta toisaalta taas akkutuotanto kuluttaa ja tuhoaa ympäristöä monin tavoin.Yksi tärkeimmistä tavoista säästää sähköä tietoteknisten laitteiden käytössä,

on valistaa käyttäjiä oikeaoppiseen toimintakulttuuriin. Luonnollisesti on monia muitakin keinoja vähentää päästöjä ja ympäristötuhoa kuin sähkön säästäminen.

Tietoteknisten laitteiden valmistaminen aiheuttaa runsaasti päästöjä ja kuluttaa luonnon varoja sekä ympäristöä. Tietoteknisten laitteiden hankintaan tulee kiinnittää huomiota ja hankkia vain tarpeeseen laitteita. Laitteiden teho pitäisi olla käyttötarpeen mukainen, eikä esim. ylimitoitettuja tehomyllyjä kannata hankkia toimistokäyttöön. Työntekijöille yleensä riittää yhden laitteen malli. Työvälineet tehtävien mukaan, ei statuksen mukaan.

Laitteiden hankinnoissa ja valinnoissa kannattaa huomioida energiatehokkuusstandardit ja merkinnät laitteissa. Yleisimpiä merkintöjä IT-laitteissa ovat perinteisesti olleet mm: Energy Star ja TCO. Monissa kodinkoneissa tulee nykyisin olla energiamerkinnät. Nykyinen energiamerkintäjärjestelmä luokittelee laitteet A:sta G:hen (A=paras), tosin se ei kata kaikkia laiteryhmiä, kuten ei välttämättä myöskään tietokoneita. Käytöstä poistetut laitteet tulee kierrättää oikeaoppisesti ja rajalliset materiaalit tulee ottaa uusiokäyttöön. ICT-asiantuntijoilla ja johdolla on organisaatioissa ratkaisevan tärkeä ja vastuullinen rooli maailmanlaajuisessa vihreässä siirtymässä.

Tässä työssä kiinnitettiin huomiota mm. *sähkön säästöön* tietokoneluokan työasemien käytössä. Virranhallintaominaisuuksia sopivasti säätämällä ja työasemien automaattisilla sammutuksilla saadaan säästöjä aikaan. Tämän lisäksi työssä hyödynnettiin käytettyä, mutta vielä toimivaa palvelinta siten, että sen *elinkaarta jatketaan* vaihtamalla siinä olevat perinteiset kovalevyt uusiin SSD-levyihin. Tällä menetelmällä saadaan testattua mahdollisesti tulevan hallintaympäristön toimivuus luokkaympäristössä ilman isoja laiteinvestointeja. Toisaalta huono asia virransäästön kannalta lienee se, että palvelimen raudan ollessa hiukan vanhempaa, niin sen energiatehokkuus ei useinkaan yllä uusimpien palvelimien tasolle. [48]

6.1 Työasemien virransäästömäärittelyt

Työasemien virransäästömäärittelyissä tehdään usein kompromissi tietoturvan kanssa, koska käyttöjärjestelmän ja ohjelmistojen päivitykset vaativat, että työasemat ovat verkossa ja päällä. Toisaalta tietokoneen ollessa jatkuvasti päällä ja verkossa, se altistuu tällöin verkon kautta tuleville mahdollisille uhkille. Eräs kompromissiratkaisu tähän ongelmaan voisi olla sellainen, että päivitykset hoidettaisiin sovituissa *huoltoikkunoissa*, esim. kerran viikossa. Tällöin työasemia ei tarvitse pitää päällä jatkuvasti. Nykyisin on tarjolla monenlaisia etäkäynnistys- ja etäsammutusratkaisuja, joilla voidaan hoitaa työasemien päivitykset ja lopuksi sammuttaa työasemat. [48]

Nykyisin monissa sähkölaitteissa ja tietokoneissa on kehittyneet *virransäästöominaisuudet* ja niitä on syytä hyödyntää. Virranhallinta-asetukset työasemissa voidaan esim. Active Directoryn ryhmäkäytäntöjen avulla asettaa järkevälle sähköä säästävälle tasolle.

Käyttäjiä tulee ohjeistaa, kuinka työasemia käytetään vastuullisesti eli milloin ne käynnistetään ja sammutetaan. Nyrkkisääntönä esim. voisi olla että, sammutetaan työasema silloin, kun sitä ei kahteen tuntiin tarvita. Toisaalta, mikäli käytetään sopivia keskitettyjä virransäästöasetuksia, niin sillä saadaan jo hyvää aikaiseksi. Perusajatuksena voidaan pitää myös, että työasemat sammutetaan aina työpäivän päätteeksi, ellei IT-osasto toisin määrää. [48]

Tässä työssä työasemille määriteltiin kerran viikossa (ke) ns. *huoltoikkuna*, jolloin työasemat käynnistyvät aikaisin aamulla BIOS:n herättämänä. Tämä siksi, jotta Microsoftin päivitykset saadaan ladatuksi työasemille valmiiksi ja ne voidaan päivittää halututtuna ajankohtana heti aamulla. Työasemille on varmuuden vuoksi ajastettu paikallisesti sammutukset työpäivän päätteeksi, mikäli käyttäjä jostain syystä unohtaisi sammuttaa itse työasemansa. Lisäksi virranhallinta-asetukset on määritelty järkevälle tasolle käytön mukaan. [48]

6.2 Palvelinympäristön energiatehokkuus

Palvelinkeskuksien lukumäärät kasvavat kiihtyvällä vauhdilla ja digitalisaatio etenee maailmanlaajuisesti. *Palvelinkeskukset ja tietoliikenneverkko* tuottavat suurimman osan internetin käytön aiheuttamista päästöistä. Ilmastonmuutoksen kannalta palvelinkeskuksien vaikutukset ylittävät jo lentoliikenteen vaikutukset. Palvelinympäristön energiatehokkuuteen vaikuttavia tekijöitä ovat mm. palvelinteknologian energiatehokkuus, virtualisoinnin vaikutukset energiatehokkuuteen, konesalipalvelujen energiatehokkuus ja optimointi.

Palvelimien tarkoitus on tarjota palveluita turvallisesti, laadukkaasti, vakaasti ja katkeamattomasti. Tämä vaatii erityisen turvatun ympäristön palvelimille, jotta palveluiden jatkuvuus voidaan taata. Kustannuspoliittisesti palvelimien pakkaustiheyden eli laskentatehon tulee olla mahdollisimman suuri, josta seuraa laitteiden voimakas kuumentuminen. Tästä johtuen tarvitaan tehokkaita jäähdytysjärjestelmiä, jotka pitävät ympäristön toimintakelpoisena. Nämä kaikki kuluttavat runsaasti energiaa ja sähköä. Jäähdytyksen sähkönkulutus voi olla jopa 30-50% konesalin koko sähkönkulutuksesta. Tehostamalla konesalin energiankäyttöä, voidaan sähkönkulutus jopa puolittaa. Tärkeimpiä keinoja tähän ovat mm. [49]

- palvelinten käytön optimointi ja virtualisointi
- palvelinten sijoittelu ja valaistuksen ohjaus
- energiatehokkaiden laitteiden ja komponenttien käyttäminen
- jäähdytysjärjestelmän ja UPS-järjestelmän optimointi
- lämpötilan optimointi ja hukkalämmön talteenotto
- vapaajäähdytyksen käyttäminen
- ilman kosteuden hallinta ja valvonta
- optimoidun ohjelmakoodin käyttäminen.

Viime aikoina on alettua puhua *ympäristöystävällisestä koodauksesta*, jossa ohjelmakoodia **optimoidaan** siten, että se kuluttaa mahdollisimman vähän dataa ja laitekapasiteettia. Optimoitu ”softa” kuluttaa vähemmän laiteresursseja ja operointikustannuksia, tällöin säästyy sähköä ja päästötkin ovat alhaisempia.

Optimoinnin merkitys ohjelmoinnissa ja palveluiden kehittämisessä tulee kasvamaan lähitulevaisuudessa. Verkkopalvelujen pystytyksessä kannattaa myös huomioida verkkokaistan käyttö siten, että se on optimaalinen käytön ja kulutuksen mukaan.

Video- ja kuvatiedostot kuluttavat kaistaa eniten ja niihin tulee kiinnittää enemmän huomioita. Videoiden osuus internet-liikenteestä on jo runsaat 80 % koko verkkoliikenteestä. Vuonna 2019 arvioitiin, että kahden tunnin elokuvan katsominen suoratoistopalvelusta kuluttaisi energiaa 1,13 kWh ja tuottaa esim. Britannian sähkötuotantorakenteella yli 300 g hiilidioksidipäästöjä. **Elokuvan katseleminen** korkeimmalla ja tarkimmalla teräväpiirtoasetuksella kuluttaa nelinkertaisen määrän keskilaatuun verrattuna. Herää kysymys, että onko se kaikki tarkoituksenmukaista liikennettä ja voisiko omaakin ruutuaikaa hiukan säännöstellä.

6.3 Ympäristöjärjestelmät ja Green ICT

Ympäristöasioiden hallintajärjestelmien tarkoitus on ohjata organisaatioita kohti ympäristöarvoja kunnioittavampaan toimintakulttuurin suuntaan. Periaatteessa ympäristöjärjestelmien käyttöönotto on vielä pääsääntöisesti vapaaehtoista organisaatioille, mutta käytännössä niiden merkitys ja painoarvo tulee kasvamaan dramaattisesti. Tämä tarkoittaa sitä, että mikäli organisaatio ei kunnioita ympäristöarvoja ja noudata tiettyjä eettisiä käytäntöjä toimissaan, niin sillä ei ole käytännössä toimintaedellytyksiä tulevaisuudessa.

Ympäristöön liittyvien asioiden hoitaminen on läheistä sukua muille toimintajärjestelmille kuten esim. **ISO 9001** laatujärjestelmälle. Näiden järjestelmien avulla voidaan saavuttaa runsaasti myös liiketoiminnallisia hyötyjä esim. kustannustehokkuuden parantuessa. Kuitenkin mielestäni ne ovat suuressa kuvassa sivuseikkoja, koska vastuullisuus ja ympäristön suojelu lienee kaikista tärkein arvo.

Ympäristöasioiden hallintajärjestelmistä tunnetuin malli maailmalla lienee standardi **ISO 14001**. Hallintamallin avulla organisaatiot voivat kokonaisvaltaisesti ja tavoitteellisesti parantaa ympäristöpoliittisten asioidensa hoitoa ja hallintaa sekä

edistää kestävää kehitystä. Standardia voidaan soveltaa kaikenkokoisille organisaatioille ja eri toimialueille. Viimeisin päivitetty versio standardista lienee vuodelta 2015. Maailmalla sadat tuhannet organisaatiot ovat ottaneet sen jo käyttöön. [50]

Organisaatioilla on mahdollista saada *ympäristösertifikaatti*, mikäli se on luonut ympäristöohjelman standardin pohjalta ja tavoitteellisesti eri parannustoimenpiteillä täyttää asetetut kriteerit ja on sisäisten ja ulkoisten auditointien avulla todennettu. Eräs suosittu suomalainen kevennetty ympäristöjohtamisen työkalu myös ISO 14001 standardin pohjalta lienee **Ekokompassi**. Se on myös Niemikotisäätiöllä käytössä ja sertifioituna. [51]

Eurooppalainen **EMAS** (the Eco-Management and Audit Scheme) ympäristöasioiden johtamisjärjestelmä sopii myös kaikille organisaatioille toimialasta riippumatta. EMAS pohjautuu samaan ISO 14001 standardiin. Järjestelmä on ulkopuolisen tahon vahvistama. [52]

WWF:n Green Office tarjoaa välineitä ympäristöjärjestelmän rakentamiseen organisaatioille. Sen avulla voi luoda oman ympäristöstrategian ja suunnitelman pienentääkseen hiilijalanjälkeään ja vähentääkseen haitallisia ympäristövaikutuksia. Järjestelmään voi asettaa vuotuiset tavoitteet ja mitata niitä. Ympäristöjärjestelmän valmistuttua, voi sen auditoida ja saada virallisen sertifikaatin. [53]

Yhtä kaikki, näiden vapaaehtoisten ympäristöhallintajärjestelmien pyrkimys on ohjata organisaatioita luonnon varojen kestävään käyttöön, vastuullisuuteen ja avoimuuteen sekä hyvinvoinnin lisäämiseen koko organisaation viitekehyksessä. Nykyisin ja varsinkin tulevaisuudessa ICT-sektorin ja teknologian painoarvo tulee nousemaan merkittävään asemaan kaikissa ympäristöpoliittisissa ongelmien ratkaisuissa ja ns. vihreässä siirtymässä.

Green ICT

Green ICT -hankkeita on käynnistynyt alkaneella vuosikymmenellä mm. Euroopassa ja Suomessa. Liikenne- ja viestintäministeriössä asetettiin vuoden 2019

loppupuolella työryhmä tieto- ja viestintäteknologia-alan ilmasto- ja ympäristöstrategian laatimiseksi. Työryhmän tehtävänä oli muodostaa yhteinen näkemys *ICT-alan ilmasto- ja ympäristövaikutuksista* Suomessa sekä suositella keinoja vaikutusten hallitsemiseksi. Tietoyhteiskunnan kehittämiskeskuksen toimesta (TIEKE) on myös käynnistynyt Green ICT -hanke. TIEKE, TIVIA ja LUT luotsaavat vuosina 2021-2023 Green ICT -hanketta, jonka tarkoitus on edistää vähähiilisempää digipalvelutuotantoa. [54] [55]

ICT-ala tuottaa paljon päästövähennyksiä edistäviä ratkaisuja, mutta samalla on kiinnitettävä huomiota alan oman hiilijalanjälkeen ja muihin ympäristövaikutuksiin. ICT-infrastruktuurin rakentamiseen liittyviin ilmasto- ja ympäristökuormituksiin tulee kiinnittää jatkossa enemmän huomiota. Yleisesti on arvioitu, että ICT-alan osuus maailman energiakulutuksesta on luokkaa 4-10% ja hiilidioksidipäästöt 3-5%. Päästöjen suuruudet riippuvat paljolti käytetyistä sähköntuotannon lähteistä. Muita toimenpiteitä tarvitaan myös mm. kiertotalouden kehittämiseen, materiaalivirtojen hallitsemiseen ja laitteiden elinkaaren pituuden kasvattamiseen.

Ihmiskunta on viimeisen sadan vuoden aikana tuhonnut oman elinympäristönsä ja siinä sivussa sotkenut koko planeetan ekosysteemin melko totaalisesti. Maailmalla on kuitenkin hiljakseen alettu ymmärtämään, että ihmisen aiheuttama ilmastonmuutos ja luonnon monimuotoisuuden hävittäminen johtaa koko planeetan elinympäristöjen tuhoutumiseen. Toimeen on onneksi jo paikoin ryhdytty, mutta riittääkö se? Alkanut vuosikymmen (v.2020-2030) näyttelee pääroolia ihmiskunnan ja koko planeetan historiassa, siinä millaisen elinympäristön tulevaisuudessa saamme tai menetämme. Siksi on tärkeätä, että digitaalistuvassa ja sähköistyvässä maailmassa jokainen toimija ja käyttäjä ottaa vastuun siitä, kuinka isoksi oma elämänsä aikainen hiilijalanjälki ja myös digitaalinen hiilijalanjälki tulee muodostumaan.

Tarina on hyvä päättää **Sir David Attenboroughin** sanoihin: *”Me olemme ensimmäinen sukupolvi, joka on todella tiedostanut ongelman – ja viimeinen, jolla on mahdollisuus tehdä asialle jotain.”* [56]

7 Yhteenveto

Työn tarkoituksena oli kehittää perinteisen tietokoneluokan tietoteknistä opetus- ja käyttöympäristöä. Standalone-työasemien kytkeminen paikalliseen toimialueeseen helpottaa työasemien hallintaa jatkossa ja samalla käyttäjien profiilien manuaaliset puhdistustyöt työasemilla jäävät historiaan.

Käyttöjärjestelmien asetukset ja määritykset työasemilla voidaan jatkossa tehdä keskitetysti Active Directoryn ryhmäkäytännöillä. Koulutusympäristön tietoturva ja tietosuoja koheni, koska jokaisella käyttäjällä on jatkossa henkilökohtainen käyttäjätunnus. Käyttäjät voivat tallentaa omiin verkossa oleviin kotikansioihinsa tekemänsä harjoitustyöt, eikä sekaannuksia niissä pääse syntymään. Tiedostoista otetaan säännöllisesti varmistuksia, jolloin tiedostojen tietoturva on paremmalla tasolla kuin ennen. Opetusmateriaalin jakaminen tapahtuu jatkossa kätevästi jakokansioiden avulla halutulla tavalla. Kouluttajalla on myös mahdollisuus tarkistaa tehdyt harjoitustyöt helposti verkon kautta omalta työasemaltaan.

Kehitystyön sivujuonteena oli saada samalla rakennettua yleistä opetusmateriaalia tieto- ja viestintätekniikan perusopiskelijoille. Palvelininfrastruktuuriin liittyviä asioita on kuitenkin runsaasti, joten vaarana oli, että työselosteesta tulisi liian laaja-alainen, vaikkakin keskiössä olisi vain Active Directory ja sen käyttöönotto. Pidin kuitenkin asiaan kuuluvana lisätä työselosteeseen joitakin mielestäni tärkeitä aihealueeseen liittyviä seikkoja, jotka eivät suoranaisesti liity Active Directoryn käyttöönottoon. Poistin kuitenkin kompromissina alkuperäisestä työselosteesta paljon tietoturvaan ja verkkoympäristöön liittyviä tärkeitäkin osa-alueita pois. En kuitenkaan voinut olla lisäämättä viimeistä kappaletta, joka liittyy ympäristöarvoihin ja energiansäästöön ICT-sektorilla, johtuen sen tärkeästä painoarvosta nykyisin.

Kehitystyö onnistui teknisesti kohtuullisen hyvin ja uusi ympäristö on nyt tuotantokäytössä. Active Directoryn ja palvelinympäristön ominaisuuksia tullaan hyödyntämään monipuolisesti koulutusympäristössä. Kaikille käyttäjille tarjotaan mm. varmistetut kotikansiot ja ryhmäkäytäntöjä hyödynnetään monipuolisesti

tarpeen mukaan. Autenttinen Active Directory -ympäristö on myös omiaan itse hakemistopalvelun koulutus- ja oppimisympäristönä. Luokkaympäristö muodostuu tällä hetkellä kymmenestä Active Directoryyn liitetyistä työasemasta ja muutamasta paikallisesta erikoistyöasemasta, joita ei ole liitetty toimialueeseen.

Tietokonesalin käyttö- ja koulutusympäristöä tullaan todennäköisesti jatkokehittämään siten, että hankitaan uusi palvelin toiseksi ohjainkoneeksi toimialueelle. Lisäksi nykyisen palvelimen käyttöjärjestelmä Windows 2016 Server Standard tullaan päivittämään uudempaan Windows 2019 Server Standard -versioon viimeistään ennen Microsoftin tuen päättymistä. Tällöin järjestelmän elinkaarta saadaan jatketuksi pidemmälle tulevaisuuteen ja vikasietoisuus toimialueella selkeästi myös paranee.

Tämä yhden miehen kehitystyöprojekti valmistui vakavan maailmanlaajuisen pandemian vallitessa ja raportin loppuosa kirjoitettiin sodan varjossa.

Lähteet

1 Niemikotisäätiö, https://niemikoti.fi/.

2 Wikipedia.org:Active Directory https://en.wikipedia.org/wiki/Active_Directory, Hakupäivä 24.1.2022.

3 Microsoft, 01/11/2022, https://docs.microsoft.com/en-us/windows-server/identity/identity-and-access, Hakupäivä 24.1.2022.

4 Francis Dishan, 2019 Mastering Active Directory Second Edition, UK, Packt.

5 Microsoft, 01/11/2022, https://docs.microsoft.com/en-us/windows-server/identity/ad-ds/get-started/virtual-dc/active-directory-domain-services-overview, Hakupäivä 27.1.2022.

6 Microsoft, 12.1.2021 https://docs.microsoft.com/en-us/troubleshoot/windows-server/identity/fsmo-roles, Hakupäivä 27.1.2022.

7 Microsoft, 24.9.2021, https://docs.microsoft.com/en-us/troubleshoot/windows-server/identity/fsmo-placement-and-optimization-on-ad-dcs, Hakupäivä 29.1.2022.

8 Microsoft, 4.12.2017, https://techcommunity.microsoft.com/t5/ask-the-directory-services-team/ese-deep-dive-part-1-the-anatomy-of-an-ese-database/ba-p/400496, Hakupäivä 29.1.2022.

9 Microsoft, https://azure.microsoft.com/en-us/overview/what-is-cloud-computing/#benefits, Hakupäivä 2.3.2022.

10 IBM, 19.6.2019, https://www.ibm.com/cloud/learn/virtualization-a-complete-guide, Hakupäivä 29.1.2022.

11 Wikipedia, https://en.wikipedia.org/wiki/Cloud_computing, Hakupäivä 29.1.2022.

12 Microsoft, 5.2.2022, https://docs.microsoft.com/en-us/azure/active-directory/fundamentals/active-directory-compare-azure-ad-to-ad, Hakupäivä 2.3.2022.

13 Dell, https://www.dell.com/support/manuals/fi-fi/poweredge-t320/t320ownersmanual/technical-specifications?guid=guid-

e8bdfcc6-3ab0-4ca0-ae9b-d1c76a959dcc&lang=en-us, Hakupäivä 29.1.2022.

14 Microsoft, 2022, https://www.microsoft.com/en-us/windows-server/pricing, Hakupäivä 29.1.2022.

15 Wikipedia, https://fi.wikipedia.org/wiki/DNS, Hakupäivä 29.1.2022.

16 Microsoft, 29.7.2021, https://docs.microsoft.com/en-us/windows-server/identity/ad-ds/plan/active-directory-integrated-dns-zones, Hakupäivä 29.1.2022.

17 Microsoft, 29.7.2022, https://docs.microsoft.com/en-us/windows-server/networking/core-network-guide/cncg/server-certs/server-certificate-deployment-overview, Hakupäivä 29.1.2022.

18 Microsoft, 20.4.2021, https://docs.microsoft.com/fi-fi/windows-server/identity/ad-fs/ad-fs-overview, Hakupäivä 29.1.2022.

19 Microsoft, 31.8.2016, https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2012-r2-and-2012/hh831593(v=ws.11), Hakupäivä 29.1.2022.

20 Microsoft, 31.8.2016, https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2012-r2-and-2012/hh831364(v=ws.11), Hakupäivä 29.1.2022.

21 Wikipedia, https://en.wikipedia.org/wiki/Dynamic_Host_Configuration_Protocol, Hakupäivä 29.1.2022.

22 Microsoft, 11.8.2021, https://docs.microsoft.com/fi-fi/services-hub/health/remediation-steps-ad/configure-the-root-pdc-with-an-authoritative-time-source-and-avoid-widespread-time-skew, Hakupäivä 30.1.2022.

23 Microsoft, 12.3.2021, https://docs.microsoft.com/en-us/windows/security/identity-protection/access-control/active-directory-security-groups, Hakupäivä 30.1.2022.

24 Kuittinen Tuomas, 2018, Active Directoryn suunnittelu ja käyttöönotto pienyrityksessä, Opinnäytetyö, Karelia-Ammattikorkeakoulu.

25 Microsoft, 17.8.2020, https://docs.microsoft.com/en-us/windows/win32/ad/naming-properties, Hakupäivä 30.1.2022.

26 Server Academy, 29.6.2021, https://www.serveracademy.com/tutorials/how-to-enable-advanced-features-in-active-directory/, Hakupäivä 30.1.2022.

27 Activedirectorypro.com, 2018, https://activedirectorypro.com/how-to-use-rsop-to-check-and-troubleshoot-group-policy-settings/, Hakupäivä 2.3.2022.

28 Activedirectorypro.com, 2021, https://activedirectorypro.com/gpresult-tool/, Hakupäivä 2.3.2022.

29 Activedirectorypro.com, 2021, https://activedirectorypro.com/gpupdate-command/, Hakupäivä 2.3.2022.

30 Wikipedia, https://en.wikipedia.org/wiki/Network-attached_storage, Hakupäivä 2.3.2022.

31 Wikipedia, https://en.wikipedia.org/wiki/Server_Message_Block, Hakupäivä 7.5.2022.

32 Dell Technologies, 2020, https://www.dell.com/support/kbdoc/fi-fi/000137238/windowsin-tiedostojen-ja-kansioiden-käyttöoikeudet.

33 Microsoft, 10.8.2021, https://docs.microsoft.com/en-us/windows-server/storage/file-server/volume-shadow-copy-service, Hakupäivä 2.3.2022.

34 Microsoft, 1.6.2021, https://docs.microsoft.com/en-us/windows/win32/dfs/distributed-file-system, Hakupäivä 2.3.2022.

35 Microsoft, 29.7.2021, https://docs.microsoft.com/en-us/windows-server/storage/fsrm/fsrm-overview, Hakupäivä 4.3.2022.

36 Morimoto Rand, 2017, Windows Server 2016 Unleashed, USA, Pearson Education.

37 Microsoft, 31.8.2016, https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2012-r2-and-2012/dn789196(v=ws.11), Hakupäivä 4.3.2022.

38 Microsoft, 31.8.2016, https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2012-r2-and-2012/dn581922(v=ws.11), Hakupäivä 4.3.2022.

39 Tyni Jarno, 2019, Konesalin suunnittelu ja toteutus, Opinnäytetyö, Hämeen Ammattikorkeakoulu.

40 Wikipedia, https://fi.wikipedia.org/wiki/RAID_(tietotekniikka), Hakupäivä 6.3.2022.

41 Dell, https://www.dell.com/support/kbdoc/fi-fi/000179517/dell-poweredge-how-to-configure-the-idrac-system-management-options-on-servers, Hakupäivä 6.3.2022.

42 Microsoft, 15.1.2022, https://docs.microsoft.com/en-us/azure/security/fundamentals/management, Hakupäivä 6.3.2022.

43 UC Berkeley, https://security.berkeley.edu/education-awareness/securing-remote-desktop-rdp-system-administrators, Hakupäivä 6.3.2022.

44 Microsoft, https://www.microsoft.com/en-us/download/details.aspx?id=45520, Hakupäivä 6.3.2022.

45 Microsoft, 29.7.2021, https://www.microsoft.com/en-us/download/details.aspx?id=45520, Hakupäivä 6.3.2022.

46 nmap.org, https://nmap.org/zenmap/, Hakupäivä 6.3.2022.

47 Toivanen Juuso, 2016, Domain Controllerien varmuuskopiointi ja vikatilanteista palauttaminen, Opinnäytetyö, Kajaanin Ammattikorkeakoulu.

48 Motiva oy, 2010, Selvitys työasemaympäristön sähkönsäästön mahdollisuuksista, https://www.motiva.fi/files/4424/Selvitys_IT-ympariston_sahkonsaastokeinoista.pdf.

49 Motiva oy, 2010, Energiatehokas konesali, https://www.motiva.fi/files/4828/Energiatehokas_konesali.pdf.

50 SFS, 2022, ISO 14000 Ympäristöjohtamisen standardisarja, https://sfs.fi/standardeista/tutustu-standardeihin/suositut-standardit/iso-14000-ymparistojohtamisen-standardisarja/, Hakupäivä 14.5.2022.

51 Ekokompassi, 2022, Ympäristöjärjestelmä, https://ekokompassi.fi/ymparistojarjestelma/, Hakupäivä 14.5.2022.

52 EMAS, 2022, Ympäristöhallinnon yhteinen verkkopalvelu, https://www.ymparisto.fi/emas, Hakupäivä 14.5.2022.

53 WWF, 2022, Green Office, https://wwf.fi/greenoffice/.

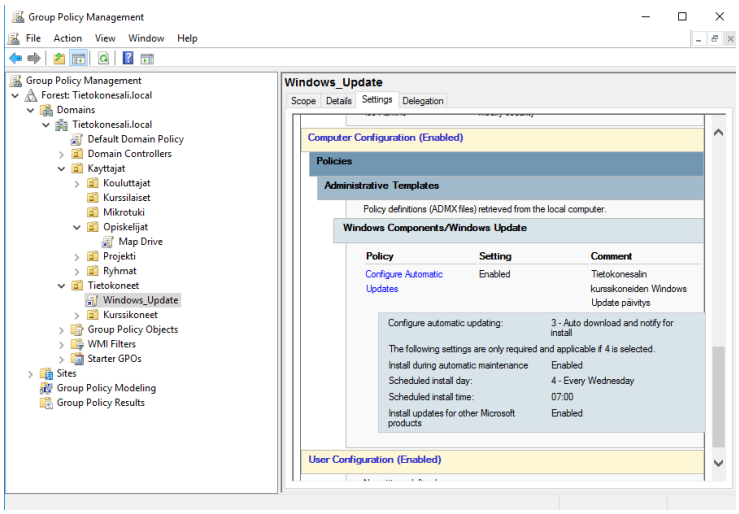
54 Liikenneministeriö, 2020, ICT-alan ilmastoja ympäristöstrategia, https://julkaisut.valtioneuvosto.fi/bitstream/handle/10024/162378/LVM_2020_12.pdf?sequence=1.

55 Tieke, 2021, Green ICT-hanke, https://tieke.fi/hankkeet/greenict-thanke/.

56 David Attenborough, Yksi elämä yksi planeetta, https://attenboroughfilm.com/about/, Hakupäivä 14.5.2022.

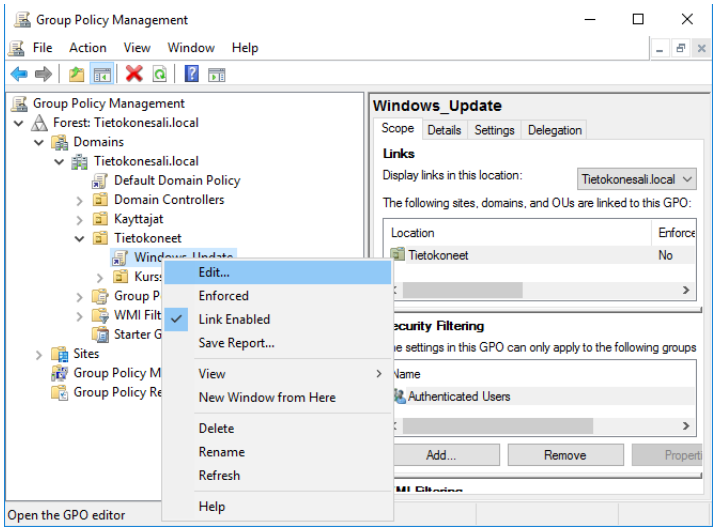
Windows päivitykset-ryhmäkäytäntö

Tässä esimerkissä käymme lävitse, miten Windows päivityksiin liittyvä ryhmäkäytäntö on luotu. Kuvassa 1 näkyy tilanne, kun ko. ryhmäkäytäntö on valittuna. Sille annettiin kuvaava nimi: **Windows_Update**.



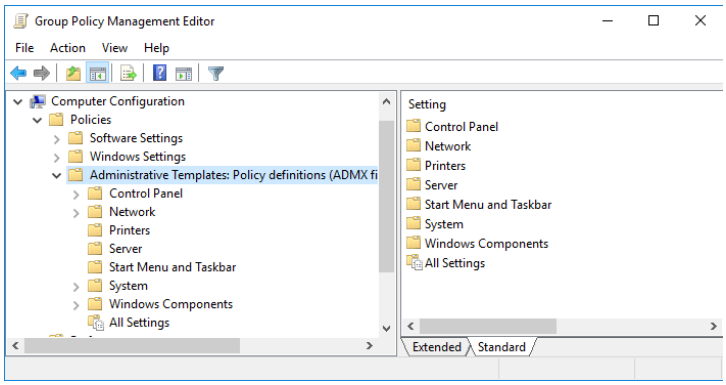
Kuva 1. Windows Update-ryhmäkäytäntö

Editointi aloitetaan kilkkaamalla hiiren oikealla painikkeella ko. ryhmäkäytännön päällä ja valitaan **Edit…**kuten kuvassa 2 esitetään.



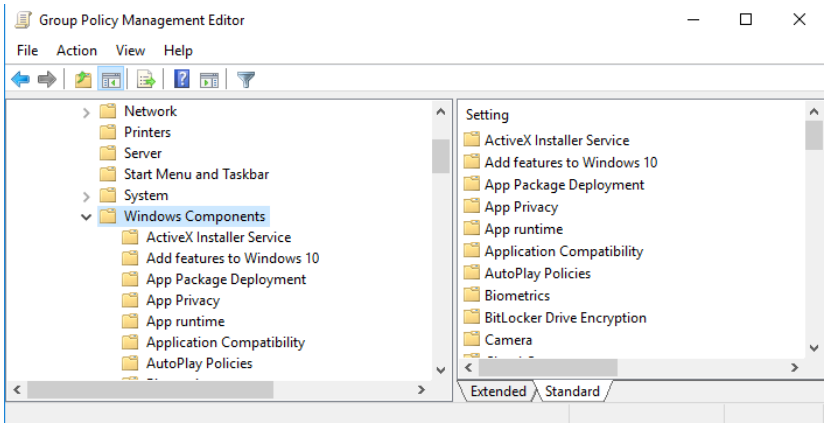
Kuva 2 Windows Update Policyn muokkaaminen

Tietokoneisiin liittyvät ryhmäkäytäntöasetukset tehdään **Computers Configuration** -haarassa. Valitaan Policies-haarasta **Administrative Templates Policy definitions** (kuva 3).



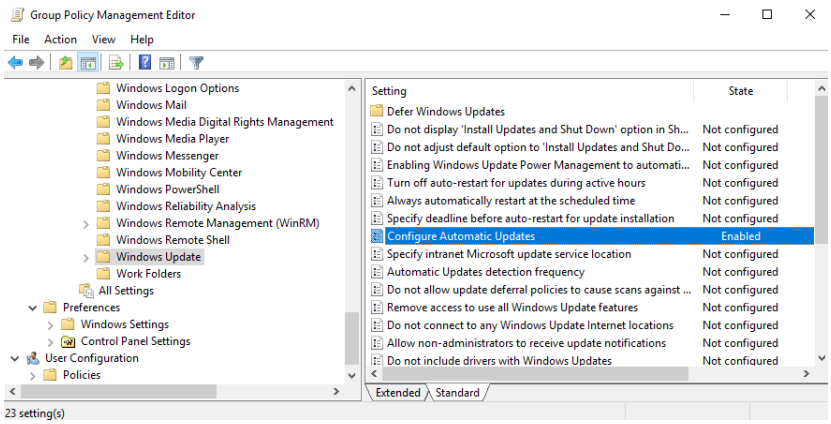
Kuva 3. Administrative Templates Policy definitions

Seuraavassa avattuna **Windows Components** -kansio, kuten kuvassa 4 esitetään:



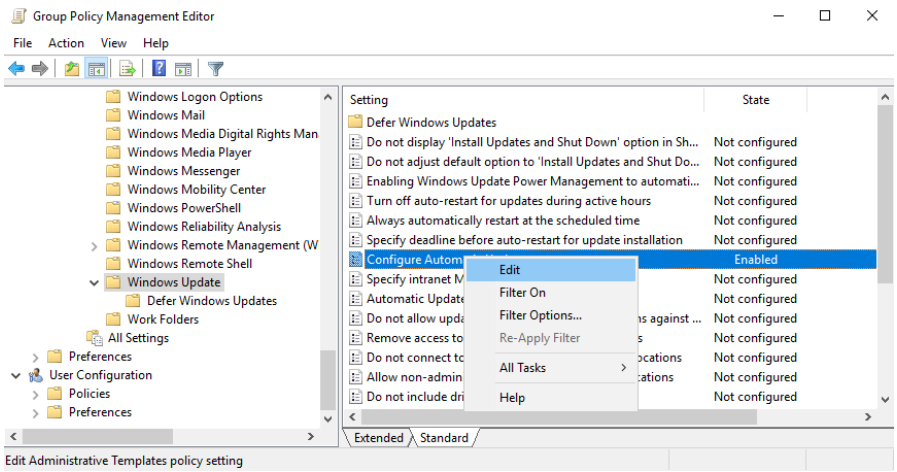
Kuva 4. Windows Components

Kansiosta Windows Components alempana on **Windows Update** -kansio, josta ko. ryhmäkäytäntö lopulta löytyy:



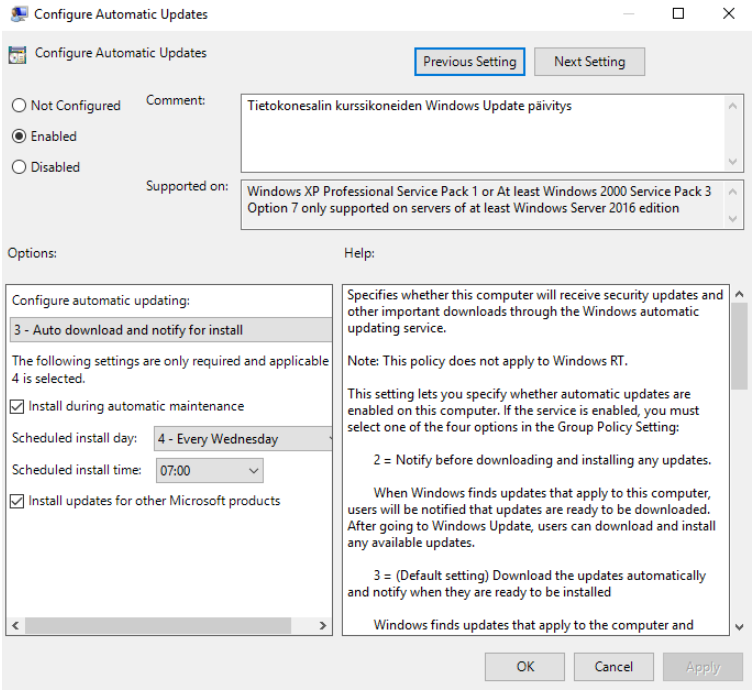
Kuva 5. Windows Update näkyy Enabled-tilassa

Editoidaan ryhmäkäytäntöä, kuten kuvassa 6 esitetään, klikataan hiiren oikealla ja valitaan **Edit**.



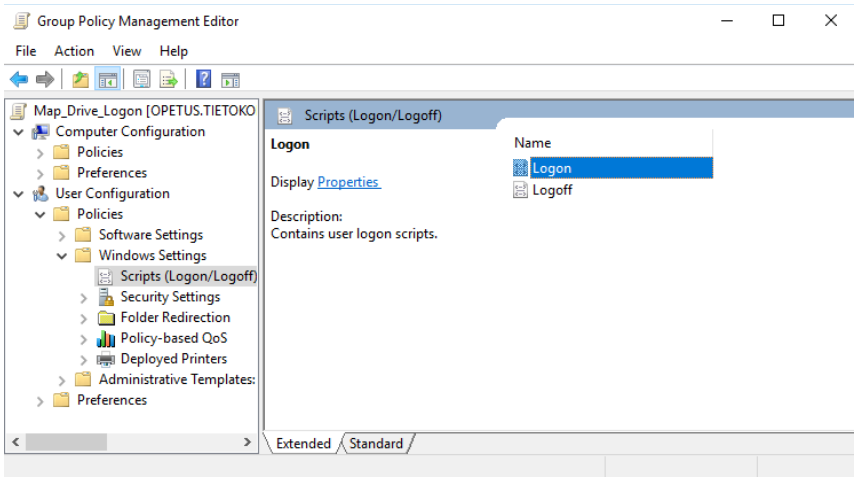
Kuva 6. Windows Update asetuksen editointi

Valitaan sopivin asetus, tässä esim. valitaan **4 - Every Wednesday** ja otetaan se käyttöön kuvassa 7 esitetyllä tavalla.



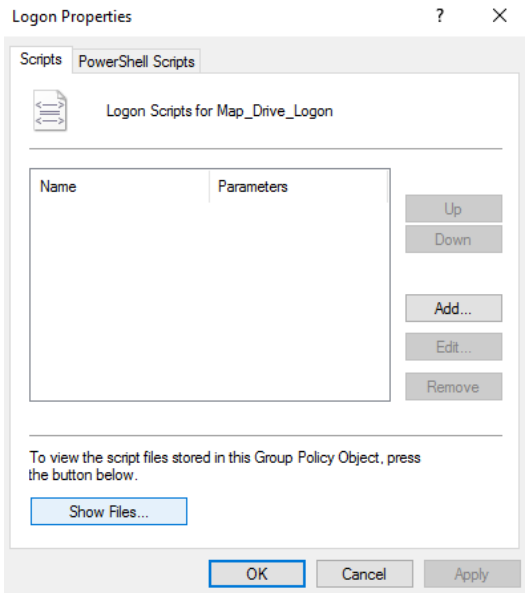
Kuva 7. Windows Update-ryhmäkäytännön asetuksien valinta ja käyttöönotto

Logon-skriptin liittäminen ryhmäkäytäntöön (Map_Drive_Logon)



Kuva 1. Map_Drive_Logon -ryhmäkäytäntö

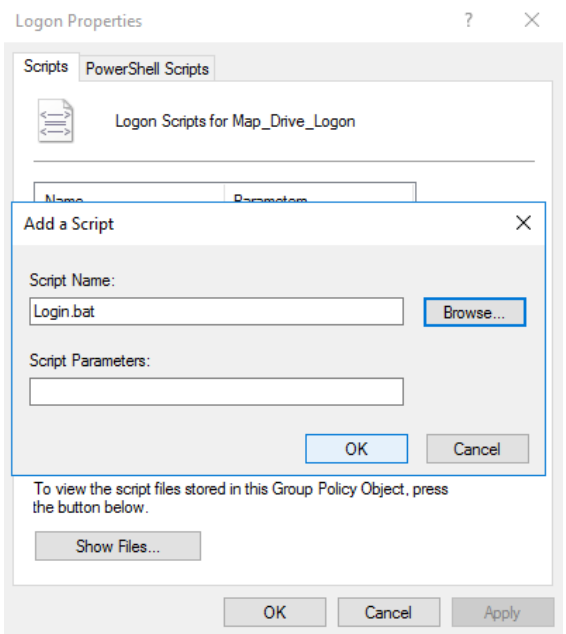
Kaksoisklikkaamalla **Logon**-säiliötä (kuva 1) avautuu **Logon Properties** -ikkuna, josta klikataan **Show Files…** painikkeesta (kuva 2), jolloin palvelimen skriptikansio avautuu. Tämä on Map_Drive_Logon -ryhmäkäytännön **Logon-tallennuskansio**. Tänne tallennetaan **Login.bat** komentojonotiedosto (kuva 3).



Kuva 2. Logon Properties

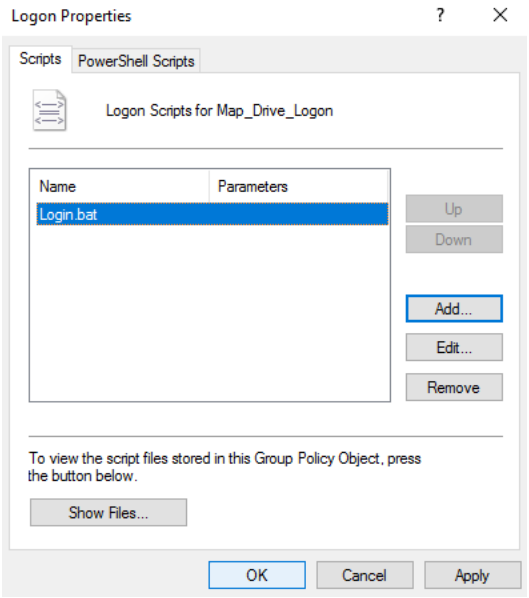
Kuva 3. Logon kansion sijainti

Tallennetaan tehty komentojonotiedosto **Login.bat** avautuneeseen kansioon ja liitetään se lopuksi **Add**-painikkeen kautta, tarvittaessa voi skriptiin lisätä lisäparametrejä, kuten kuvassa 4 näkyy.



Kuva 4 Komentojonon lisääminen

Kuitataan lopuksi **OK**-painikkeesta, jolloin tiedosto liitetään ko. ryhmäkäytäntöön (kuva 5)

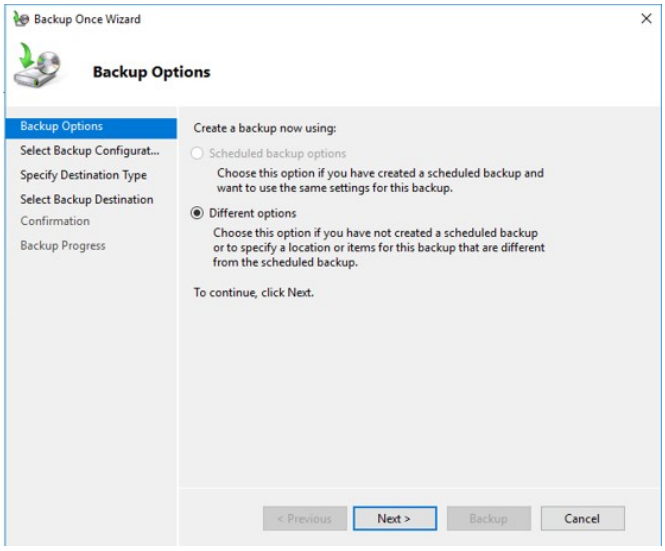


Kuva 5. Login.bat lisättynä ryhmäkäytäntöön

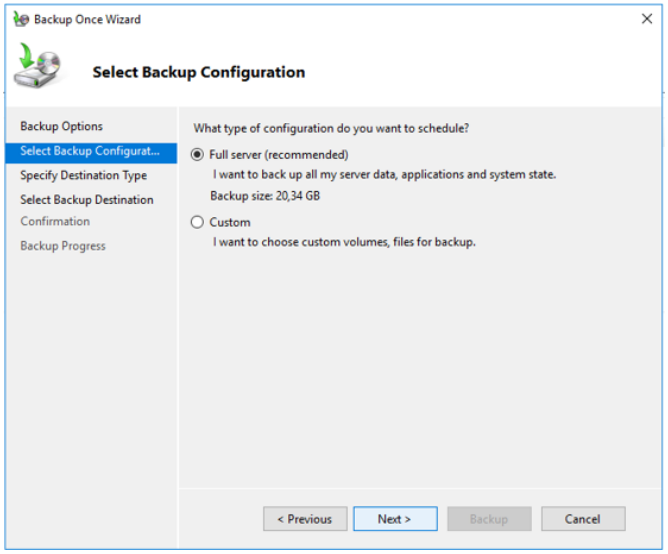
Tämän jälkeen voidaan testata ryhmäkäytännön toimivuus ennen käyttöönottoa testitunnuksella.

Palvelimen täysivarmistus esimerkki

Varmistusohjelma käynnistetään Tools-valikosta -> **Windows Server Backup**. Valitaan kertaluonteinen varmistus **Backup Once**, koska emme ole luomassa ajastettua varmistusta. Klikkaa **Next**-painiketta (kuva 1) ja valitse Täysivarmistus **Full server** (recommended). Backupin koko näkyy ohessa (kuva 2).

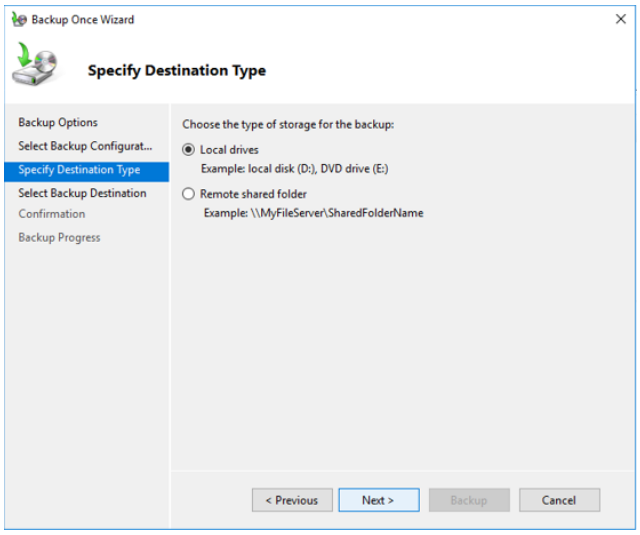


Kuva 1. Kertaluonteinen varmistus Backup Once

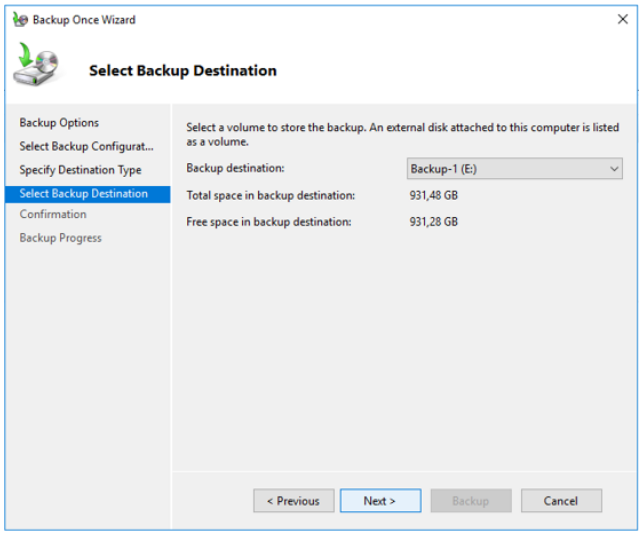


Kuva 2. Valitaan palvelimen täysi varmistus

Varmistus tallennetaan tässä palvelimessa ulkoiselle kiintolevylle, joka on esim. kytkettynä USB-väylän kautta palvelimeen eli valitaan **Local drives** (kuva 3). Ulkoisen kiintolevyn koko on 931 Gt ja se näkyy E-asemana käyttöjärjestelmässä kuvassa 4.

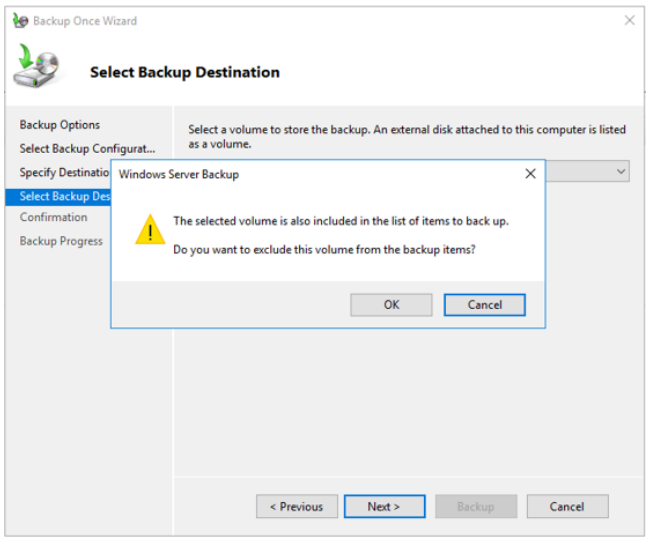


Kuva 3. Valitaan paikallinen media (USB), johon varmistus tallennetaan



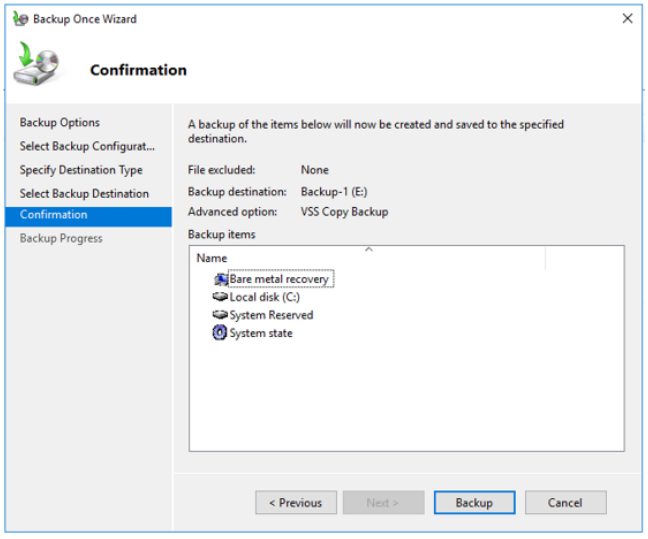
Kuva 4. Varmistuksen tallennusmedia

Varmistusohjelma kysyy: kuvassa 5, että poistetaanko ko. varmistuslevy varmistettavien listalta, jolloin vastataan myöntävästi eli klikataan **OK**-painiketta.



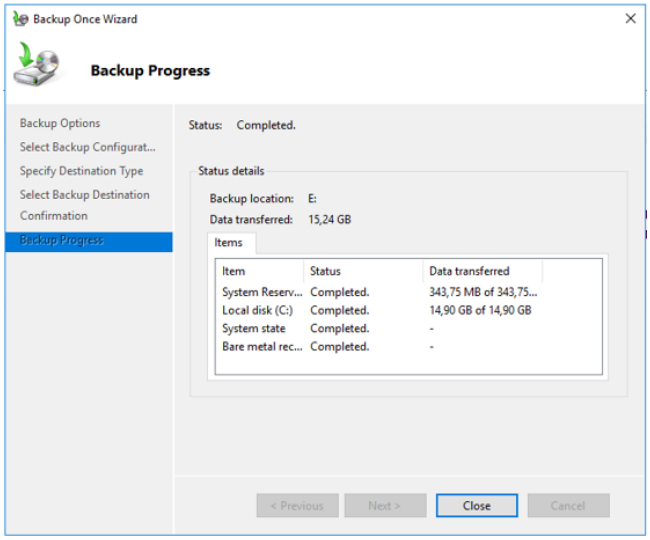
Kuva 5. Kohdelevyn eli varmistusmedian poistaminen varmistuslistalta, klikataan OK-painiketta.

Varmistusohjelma näyttää valinnat vielä koosteena kuvassa 6. Klikataan **Backup**-painiketta.



Kuva 6. Kooste valinnoista ja hyväksyntä

Varmistusohjelma käynnistyy ja näyttää ikkunassa suorituksen etenemisen. Lopuksi klikataan **Close**-painiketta ja täysivarmistus on suoritettu (kuva 7).



Kuva 7. Varmistus suoritettu ulkoiselle kiintolevylle

Edellä näytettiin periaate, miten täysivarmistus voidaan tehdä kertaluonteisesti. Kannattaa kuitenkin tutustua tarkemmin kaikkiin varmistusohjelman ominaisuuksiin ja määrittelymahdollisuuksiin. Valitsemalla varmistusohjelman alussa **Custom**-valinta, pääsee tarkemmin vaikuttamaan varmistuksien määrittelyihin. Huomioitava seikka kaikissa varmistuksissa on se, että muistaa aika ajoin testata myös **palautuksen onnistuminen**.

Sivuhuomautuksena mainittakoon, että kun automatisoidaan (ajastetaan) varmistuksia Microsoftin Backup-ohjelmalla kannattaa edetä **Custom**-valinnan kautta ja määritellä valinnat oikein liittyen mm. **VSS Full Backup -/VSS Copy Backup** -valintoihin.

Toisena sivuhuomautuksena on, mikäli halutaan automatisoida palvelimen varmistukset harvemmin kuin kerran päivässä, tulee tehdä ajastusmääritykset ensin **Microsoftin Server Backup** -ajastimella ja sen jälkeen käydä muuttamassa palvelimen **Task Schedulerin** kautta haluttu harvempi varmistussykli Backup-kansioon ilmaantuneeseen ko. varmistusprosessin triggerin asetuksiin.