Opinnäytetyö (AMK)

Tieto- ja viestintätekniikka

2021

Ossian Helmi

IT-INFRASTRUKTUURI JA SEN AUDITOINTI

TURKU AMK
TURKU UNIVERSITY OF APPLIED SCIENCES

OPINNÄYTETYÖ (AMK) | TIIVISTELMÄ

TURUN AMMATTIKORKEAKOULU

Tieto- ja Viestintätekniikan insinööri

2021 | 36 sivua, 0 liitesivua

Ossian Helmi

IT-INFRASTRUKTUURIN AUDITOINTI

Lähes kaikki organisaatiot tukeutuvat vahvasti IT-infrastruktuuriin jokapäiväisessä toiminnassaan. On tärkeää, että infrastruktuuri on suunniteltu siten, että se tukee organisaation toimintaa. Siksi organisaation tulisi auditoida infrastruktuuriaan tasaisin väliajoin varmistuakseen, että infrastruktuuri tukee organisaation toimintaa halutulla tavalla.

Organisaatioiden it-infrastruktuuri koostuu monesta osa-alueesta, joista jokainen on omalla tavallaan kriittinen. Jokainen näistä osa-alueista tuleekin tutkia läpikotaisin, jotta pystytään luomaan raportti, joka kertoo organisaatiolle sen infrastruktuurin todellisen tilan. Auditointi on laaja käsite. Tässä työssä keskitytään tekniseen auditointiin. Auditointi pohjautuu lähes kokonaan auditoijan omaan ammattitaitoon ja kokemukseen. Auditoijan oman ammattitaidon lisäksi auditoinnissa nojaudutaan vahvasti myös palveluiden ja toiminnallisuuksien parhaisiin toimintatapoihin. Parhaat toimintatavat löytyvät suoraan tutkittavan palvelun kehittäjän omasta dokumentaatiosta. Parhaiden toimintatapojen konfigurointi on aina tilanneriippuvaista.

Auditoinnin lopputuloksena on aina auditointiraportti. Raportissa käydään yksityiskohtaisesti läpi infrastruktuurin osa-alueet ja niiden konfiguraatiot. Raportissa annetaan suosituksia ja ohjeistuksia siitä, kuinka infrastruktuuria tulisi kehittää tai muuttaa. Raportti ei ole infrastruktuurin kehityssuunnitelma vaan kartoitus, josta voidaan luoda kehityssuunnitelma. Raportin tulee olla sellainen, että sen pystyy ymmärrettävästi lukemaan myös ei-teknisesti koulutettu henkilö. Auditointi ei yksinään ratkaise infrastruktuurin ongelmia. Organisaatio voi hyödyntää raporttia mahdollisissa jatkotoimenpiteissään.

ASIASANAT:

Active Directory, Auditointi, IT-infrastruktuuri

BACHELOR´S | ABSTRACT

TURKU UNIVERSITY OF APPLIED SCIENCES

Information and Communications Technology

2021 | 36

Ossian Helmi

AUDITING WINDOWS IT-INFRASTRUCTURE

Nowadays almost all organizations rely heavily on Windows Active Directory and its services to run their infrastructure. That's why it is important to keep that infrastructure running as well as possible and make sure it supports the organizations business as well as possible. That's where auditing the infrastructure comes into play. Auditing the infrastructure is a key element in making sure that the infrastructure is running as it can and gives the organization maximal return on investment.

Each organization has its own unique IT-infrastructure, which is an array of services, functions and physical hardware intertwined as a mesh. Every part should play a critical role to the infrastructure. Therefore, should be checked for flaws and misconfigurations at regular intervals. Auditing is a large concept starting from the users experience to physical examination of the infrastructure at hand. In this thesis I'll be focusing on the physical part of the audit.

Auditing Windows AD-infrastructure relies heavily on the knowledge and expertise of the auditor. The auditor should have a good knowledge of the best practices of all the functions and services at hand. All the background for the best practices should be from the maker of the said service or functionality. Of course, the infrastructure and its functions should be taken in consideration with the best practices. Not all best practices work in every situation and that's where the auditor's expertise comes into play.

At the end of the audit the organization should receive an audit report, which showcases all the findings about all the individual parts of the infrastructure. All the findings are explained and showed in the report. The report should also explain the severity and possible problems with the findings. The report should give a good understanding of all the problems in the organizations infrastructure and try to give suggestions how to fix said problem. The report itself is not a "how to fix everything" -guide. Report should bring awareness and suggestions.

KEYWORDS:

Audit, Active Directory, IT-infrastructure

SISÄLTÖ

KUVAT

KÄYTETYT LYHENTEET TAI SANASTO

AD	Active Directory. Microsoftin kehittämä käyttäjähakemistopalvelu.
DC	Domain Controller eli ohjauspalvelin. Palvelin, joka toimii käyttäjähakemiston ytimenä ja hoitaa useita tietokannan tärkeitä tehtäviä.
GPO	Group Policy Object. Käyttäjähakemistossa käytettävä asetusobjekti, jonka avulla määritetään käyttäjien ja laitteiden ominaisuuksia
PowerShell	Microsoftin komentotulkki Windows-käyttöjärjestelmille.
IP	Internet Protocol. Verkon protokolla, joka huolehtii IP-verkkopakettien toimittamisesta.
IT	Information Technology. Tieteenala., jossa korostuu tiedonsiirto, käsittely sekä internetin ymmärtäminen ja kehittäminen.
DFS	Distributed File System. Windowsin toiminnallisuus, joka mahdollistaa monilla palvelimilla olevien jaettujen tiedostojen ryhmittelyn
DHCP	Dynamic Host Configuration Protocol. Verkkoprotokolla, jonka yleisin tehtävän on jakaa IP-osoitteita lähiverkkoon kytketyille laitteille
DNS	Domain Name System. Internetin nimipalvelujärjestelmä, joka muuttaa verkkotunnuksia IP-osoitteiksi ja IP-osoitteita verkkotunnuksiksi
FSMO	Flexible Single Master Operations. Toimialueen ohjauskoneen spesialisoitu toiminnallisuus, joka takaa toimialueen toiminnallisuuden
NAS	Network-attached storage. Verkkotallennusjärjestelmä, joka jakaa tallennustilaa tietoverkossa yhteiskäyttöön.
DSMR	Directory Services Restore Mode. Toimialueen ohjauskoneen toiminnallisuus, joka mahdollistaa palvelimen irroittamisen verkosta hätätilanteissa.
Azure	Microsoftin pilvipalvelu.
URL	Uniform Resource Identifier. Merkkijono, jolla kerrotaan tietty tiedon paikka.
MAC-osoite	Media Access Control. Verkkosovittimen yksilöivä osoite.
NTP	Network Time Protocol. Täsmällisen tiedon välittämiseen tarkoitettu protokolla.

SMB	Server Message Block. Microsoftin kehittämä hajautettu levyjärjestelmä.

1 JOHDANTO

Nykyisin lähes jokaisen organisaation toiminta tukeutuu erittäin vahvasti käytössä olevaan perus-IT-infrastruktuuriin sekä siinä toimiviin erilaisiin sovelluspalveluihin ja tietojärjestelmiin. IT-infrastruktuuri on yksi keskeisimmästä, ellei jopa keskeisin toiminnan mahdollistaja. Organisaation ja IT:n suhdetta havainnollistetaan kuvassa 1.

Kuva 1: havainnollistus organisaation infrastruktuurista

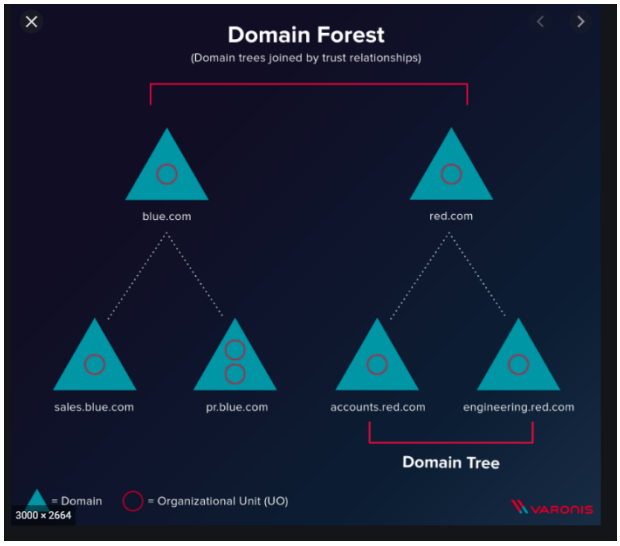
IT-infrastruktuurilla ja sen kunnolla on organisaation näkökulmasta suuri merkitys. IT-infrastruktuuri yhdessä Active Directory -palvelun kanssa on eräänlainen kivijalka, jonka päällä organisaation IT-palvelut toimivat. It-infrastruktuuri hyödyntää Active Directoryn tarjoamia palveluita. Ongelmat näiden palveluiden toiminnassa voivat aiheuttaa merkittävää haittaa ja vahinkoa yrityksen toiminnalle. Siksi onkin hyvin tärkeää, että infrastruktuuria ylläpidetään ja kehitettään koko ajan, jotta voidaan taata sen normaali toiminta.

1.1 Active Directory

Active Directory -hakemistopalvelu on koko Windows-infrastruktuurin ydin. Sen ympärille rakennetaan kaikki toiminnallisuus, mitä infrastruktuuriin luodaan. Active Directory toimii tietokantana, johon tallennetaan identiteettejä. Identiteettien säilyttämisen lisäksi Active Directoryn tehtäviin kuuluu identiteettien tunnistaminen. Tunnistamisen jälkeen Active Directoryn tehtäviin kuuluu vielä identiteettien valtuutus. Active Directory siis säilyttää identiteettejä, vastaa identiteettien tunnistamisesta sekä pitää huolta identiteettien valtuuksista. Identiteettien lisäksi Active Directoryllä on monia muita tehtäviä, kuten tapahtumien hallinta ja valvonta sekä kokoonpanojen hallinta.

Edellä mainittujen lisäksi monet palvelut, joita it-infrastruktuurissa käytetään hyödyntävät vahvasti Active Directoryä. Esimerkkinä tästä on DFS (engl. distributed filesystem) joka nojaa vahvasti Active Directoryn auktorisointi -toiminnallisuuteen. DFS käyttää auktorisointia, kun jaetaan käyttäjille tai ryhmille oikeuksia tiedostoihin tai tiedostosijainteihin. Ilman Active Directoryn tuomaa keskitettyä identiteettien hallintapalvelua olisi tiedostosijaintien ja tiedostojen tietoturvallinen jakaminen huomattavasti hankalampaa.

Active Directoryn rakenteesta ja koosta käytetään yleensä kolmea eri termiä. Metsä Active Directorystä puhuttaessa kuvastaa yhden tai useamman puun kokoelmaa. Puut ovat Active Directoryn osa-alueita, joiden alla on yksi tai enemmän toimialueita. Termeillä kuvataan helposti ja ymmärrettävästi infrastruktuurin laajuutta. Metsät ovat yhden tai useamman puun kokonaisuuksia. Metsään kuuluvien puiden välillä ei tarvitse olla fyysistä yhteyttä. Metsillä kuvataan, kuinka laaja kokonaisuus on. Toimialueita voi ajatella puiden juurina. Toimialueet ovat liitännäisiä niitä hallinnoivaan puuhun. esimerkiksi puun contoso.com toimialueita voi olla esimerkiksi palkat.contoso.com ja laskutus.contoso.com. Molemmissa toimialueissa on yhdistävänä toimialueena contoso.com puu, mutta ovat omia toimialueitaan (ks. kuva 2).



Kuva 2: Metsä, puut ja toimialueet havainnollistettuna. (Varonis)

1.2 Active Directoryn auditoinnin tavoitteet

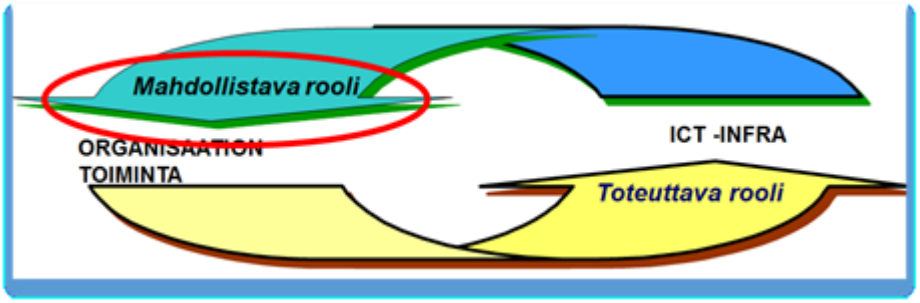
Active Directoryn auditoinnin tavoitteena on muodostaa kokonaiskuva auditoitavasta infrastruktuurista ja siihen liittyvien palveluiden nykytilasta sekä mahdollisista kehityskohteista. Eri osa-alueita tulisi tarkastella muun muassa seuraavilla tavoilla:

1. Millainen kokonaisuuden, sekä eri osa-alueiden tila on nyt.
2. Millaisia havaintoja voidaan tehdä pelkästään auditoinnin perusteella infrastruktuurin tilasta.
3. Millaisia suosituksia ja ohjeistuksia tarkastelun perusteella voidaan tehdä.

Auditoinnin lopuksi auditoinnin vastaanottajalle tehdyssä raportissa luodaan pohjaa sekä palvelin- että työasemainfrastruktuurin kehittämiselle. Raportissa on yleisiä ohjeita sekä suosituksia infrastruktuurin kehittämiseksi. Esimerkiksi DHCP:tä käsittelevässä osassa pyritään ohjeistamaan sitä, miten auditoija itse uudistaisi kyseistä osa-aluetta. Raportti ei kuitenkaan pyri olemaan varsinainen IT-infrastruktuurin kehityssuunnitelma. Raportin on tarkoitus antaa auditoidun organisaation johdolle käsitys IT-infrastruktuurin nykytilasta, sen ongelmakohdista ja tarvittavista toimenpiteistä ongelmien korjaamiseksi.

Raportti tulisikin luoda siten, että myös organisaation johto saisi selkeitä vastauksia siihen, toimiiko it-infrastruktuuri organisaation ja sen johdon odotusten mukaisesti, kuten

havainnollistettu kuvassa 3. Lisäksi tarkastellaan, onko hallinta optimoitu siten, että ylläpito toimii mahdollisimman kustannustehokkaasti. Tarkastella myös sitä, miltä AD-infrastruktuurin halutaan näyttävän lähitulevaisuudessa. Auditointiraportin tulee siis olla kokonaisuudessaan selkeä ja helppoluettava. Samaan aikaan auditointiraportti on teknisesti tarkka kirjallinen tuotos, joka viestii tarvittavat asiat selkeästi niin IT-ammattilaiselle kuin vähemmän teknisesti osaavalle henkilölle.



Kuva 3: IT:n rooli organisaatiossa

2 ACTIVE DIRECTORYN JA SEN PALVELUIDEN YLEISKUVA

Kokonaiskuva Windows palvelin -infrastruktuurin tilasta saadaan tutkimalla haluttua ympäristö. Windows-infrastruktuurin auditointiin usein kuuluu Active Directory toimialueen ohjauskone -palvelimet, tiedostopalvelimet sekä eri palveluille kuuluvat palvelimet. Sekä kaikkien edellä mainittujen toteutustavat sekä konfiguraatiot.

2.1 Yleiskuva verkossa toimivista laitteista ja palveluista

Yleiskuva verkossa toimivista laitteista saadaan helpoiten ajamalla riittävillä oikeuksilla PowerShell-komentoja eri parametrein. Näin saadaan tietoa mitä laitteita verkossa. Kaikkein tärkein vaihe on selvittää toimialueen infrastruktuurin laajuus. Se selvitetään tarkastelemalla montako metsää ja puuta toimialueella on. Puut ja metsät muodostavat koko Windows-infrastruktuurin pohjan. Näiden lisäksi on hyvä selvittää montako toimialuetta infrastruktuuri kattaa.

Tämän jälkeen voidaan alkaa tutkia, millaisia palveluita infrastruktuurissa on ja millaisessa kunnossa nämä palvelimet ovat. Esimerkiksi **komennolla Get-ADComputer -Filter {(OperatinSystem -Like ”Widows server”) -and (enabled -eq ”True”)} -Properties OperatingSystem | ft DNSHostname, OperatingSystem** saadaan PowerShell kertomaan, montako palvelinta toimialueella on. Lisäksi komento kertoo niiden järjestelmäversiot. Järjestelmäversioiden lisäksi on hyvä selvittää millä toiminallisuustasolla infrastruktuurin metsä ja puut ovat. Tästä nähdään, onko toimialueella käytössä palvelimia, jotka ovat jo poistuneet tuen piiristä eivätkä saa enää järjestelmäpäivityksiä.

Toimialueella olevien käyttäjäobjektien määrää on hyvä tutkia komennolla: **(Get -ADuser -Filter *).count**. Lisäksi voidaan tarkistaa, kuinka moni näistä käyttäjätunnuksista on aktiivisena lisäämällä filteriksi **’enabled -eq $True’**. Käyttäjätunnusten määrää olisi hyvä peilata työntekijöiden määrään. Jos tunnuksia on paljon enemmän kuin käyttäjiä, on todennäköistä, että infrassa on yhä entisten työntekijöiden tunnuksia. On tärkeää, että tarpeettomat tunnukset poistetaan asianmukaisesti. Tämä lisää tietoturvaa merkittävästi.

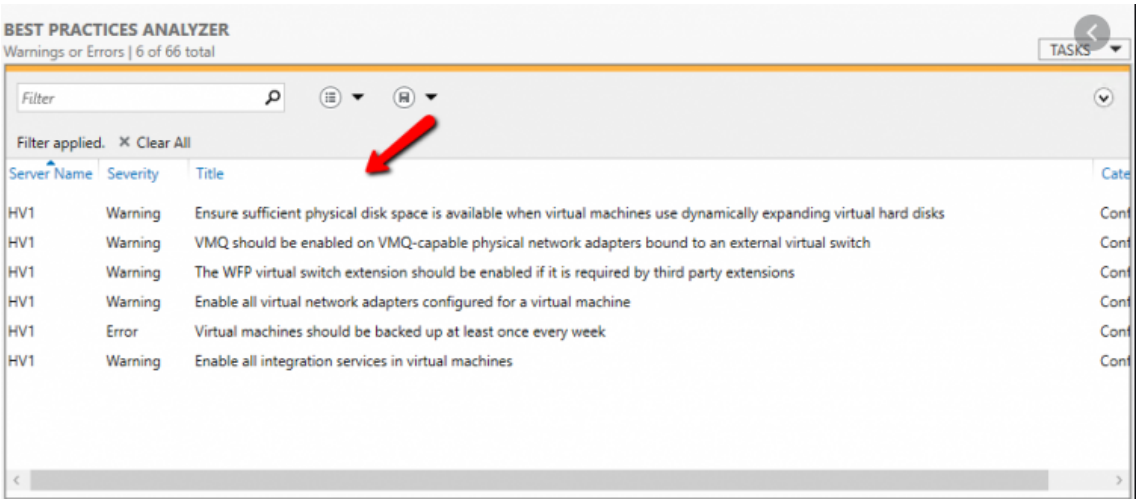
2.2 Yleiskuva

Ensimmäisenä tulisi havainnoida infrastruktuurin laajaa yleiskuvaa, jotta tiedetään, mitä ympäristöltä voidaan odottaa. Ensiarvoisen tärkeää on tutkia palvelinympäristön vikasietoisuutta. Jokaisessa ympäristössä tulisi olla vähintään kaksi toimialueen ohjauskonetta, jotta saavutetaan edes alhaisin vikasietoisuus. Lisäksi ohjauskoneiden fyysistä sijaintia tulisi arvioida vikasietoisuuden kannalta. Tätä arvioitaessa mietitään, olisiko ohjauskoneita mahdollista sijoittaa eri toimipisteisiin. Mikäli ohjauskoneet ovat samalla virtuaalialustalla, tulisi selvittää mahdollisuutta sijoittaa ohjauskoneet eri virtuaalialustoille, jottei yhden palvelimen fyysinen vika kaada koko ympäristöä.

Toimialueen ohjauskoneilta tulisi myös selvittää onko niillä käytössä Windows-palomuuri. Mikäli palomuuri on käytössä, selvitetään mitä palveluita ohjauskoneella on käytössä ja onko niille luotu tarvittavat konfiguraatiot palomuurisääntöihin. Mikäli palomuuri on poissa käytöstä, tulisi palomuuri laittaa päälle. Tämän jälkeen tulisi luoda palomuuriin ohjauskoneella toimivien palvelujen vaatimat säännöt. Lisäksi ohjauskoneiden Windows päivitysten tila tulisi tarkastaa. Tilaa tarkastettaessa tulee ottaa huomioon, onko päivitykset määritelty WSUS-palvelimen avustuksella vai haetaanko ne automaattisesti Windows päivityksen avulla. Päivitykset tulisi hoitaa keskitetysti ennalta sovitulla testaus- ja asennusprosessilla.

Active Directoryn OU-hierarkian tarkastelu yleisellä tasolla pitää sisällään objektien sijoittelua hierarkiassa. Tarkastellaan sitä, onko OU -hierarkiaan luotu ryhmittelyjä vai ovatko koneobjektit ja käyttäjät alkuperäisissä ryhmissään käyttäjät ja tietokoneet. Tämä hierarkia on hallinnan kannalta hankala ja sitä tulisi kehittää.

Alustavaa tutkimistyötä helpottamaan on monenlaisia eri työkaluja, jotka automatisoivat havaintojen tekemistä. Yksi näistä työkaluista on esimerkiksi BPA analyzer -työkalu. BPA analyzer on Windowsin oma hyvien toimintatapojen analysointityökalu. BPA analyzerin avulla saadaan helposti luettava listaus ohjauskoneella olevista konfiguraatiovirheistä tai vanhentuneista toimintatavoista (ks. kuva 4).



Kuva 4: Esimerkki BPA Analyzer -työkalun havaitsemista ongelmista. (askme4tech)

2.3 Raportointi

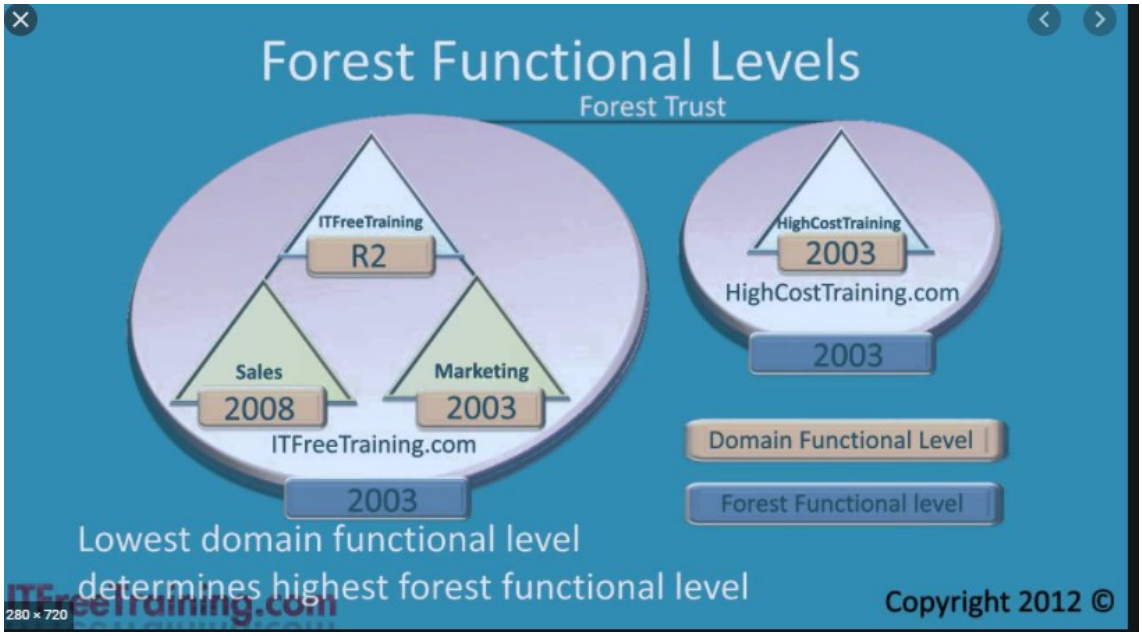
Auditointiraportin alkuvaiheessa luodaan infrastruktuurin yleiskuva. Tätä havainnointia voidaan todentaa helposti esimerkiksi kuvilla ympäristöstä. Näitä kuvia tuetaan tekstillä, mutta lukijalle annetaan mahdollisuus tulkita näkemäänsä ja ohjataan siten oikeaan suuntaan. Kuvilla vahvistetaan omia väittämiä ja raportin alussa osoitetaan, että kaikki raportoidut tiedot perustuvat faktaan. Raportin alkuvaiheessa yleisen tutkiskelun ja havainnoinnin jälkeen voidaan antaa alustavia suosituksia, joita syvennetään raportin myöhemmissä vaiheissa. Myöhemmin raportissa syvennytään tarkemmin siihen, miksi olisi suositeltavaa toimia näin.

3 ACTIVE DIRECTORY

3.1 Active Directoryn toteutus

Active Directory -hakemistopalvelu muodostaa koko Windows-infrastruktuurin ytimen, jonka ympärille kaikki muut osa-alueet ja palvelut muodostuvat. Identiteetit, joita infrastruktuurissa käytetään tallentuvat Active Directoryyn eli se toimii ympäristön identiteettivarastona. AD vastaa kaikkien näiden identiteettien tunnistamisesta eli ympäristön pääsynhallinnasta. Pääsynhallinnan lisäksi AD vastaa ympäristön identiteettien valtuutuksesta. Näiden lisäksi monet muut ympäristön palvelut hyödyntävät Active Directoryä. Näihin kuuluvat muun muassa DNS (engl. domain name system) ja DFS (engl. distributed file system). (netwrix2017a)

Active Directoryn toteutusta tutkiessa tulee ensimmäisenä selvittää, millaisesta ympäristöstä on kyse ja montako puuta ja toimialuetta on käytössä. Tämän jälkeen voidaan selvittää millä toiminnallisuustasolla puu ja toimialue ovat. Toiminnallisuustasot toimivat siten, että toiminnallisuustaso voi olla yhtä korkea kuin toimialueen alimman ohjauskoneen toiminnallisuustaso, kuten kuvassa 5. Ohjauskoneiden toiminnallisuustasoa on mahdollista laskea tarpeen mukaan.



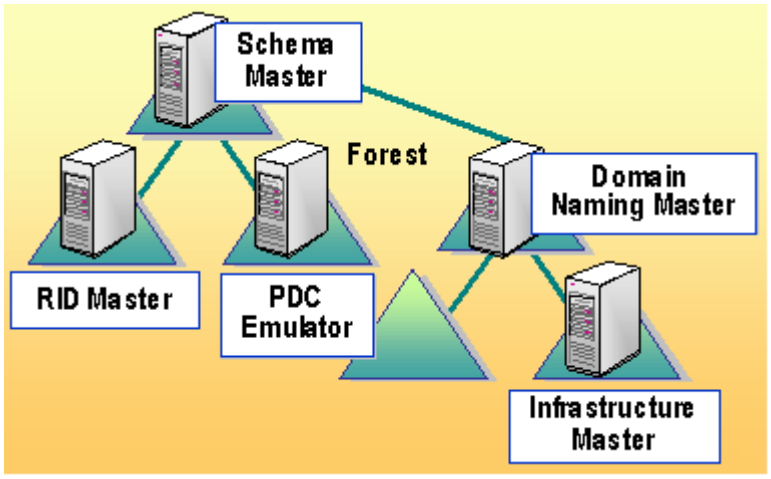
Kuva 5: Toiminnallisuustasojen havainnollistus. (Youtube, itfreetraining)

3.2 FSMO-roolit

Active Directory voi olla konfiguroitu multi-master- tai single-master-ratkaisuna. Multi-master ratkaisu tarkoittaa sitä, että toimialueen ohjauskoneet ovat keskenään saman arvoisia. Kaikissa on active Directoryn tietokannasta kirjoituskelpoinen versio ja jokaisen kautta voidaan tehdä active Directoryn tietokantaan kohdistuvia operaatioita, kuten luoda, muokata ja poistaa objekteja. Multi-master-ratkaisussa kaikki ohjauskoneet toimivat LDAP- ja Key distribution -service-palvelimina. Tämä tarkoittaa myös sitä, että infrastruktuuri on vikasietoisempi, vaikka kaikki muut paitsi yksi ohjauskoneista olisi pois pelistä. Active Directory toimii, kunnes viimeinenkin ohjauskone on pois toiminnasta. (Microsoft 2012a.)

Single-master ratkaisussa jokainen ohjauskone on omalla tavallaan kriittinen tietyille palveluille ja on täten herkempi vioille. Toinen ohjauskone ei esimerkiksi voi ottaa sammuneen ohjauskoneen roolia ilman toimenpiteitä, vaan se pitää manuaalisesti konfiguroida uuteen rooliin. On operaatioita, jotka eivät sovellu tehtäväksi multi-master -tietokannassa. Nämä operaatiot tehdään vain sen koneen kautta, jolle on konfiguroitu sitä tehtävää vastaava hallitsija rooli. (netwrix2017b)

Active Directoryn käyttöön vaaditaan 5 eri FSMO-roolia (engl. Flexible single master operations) eli joustavia yhden tekijän operaatioita. Jokainen näistä rooleista voi olla yhtäläisesti vain yhdellä toimialueen ohjauskoneella tai ne voidaan kaikki konfiguroida samalle ohjauskoneelle. Kolme viidestä FSMO-roolista ovat toimialuekohtaisia kuten kuvasta 6. Näitä ovat oman infrastruktuurin hallitsija (engl. infrastructure master), relatiivisten identiteettien hallitsija (engl. Relative identity master) sekä primäärisen toimialueen ohjauskoneen hallitsija (engl. Primary domain controller master). Lisäksi kaksi näistä viidestä FSMO-roolista ovat metsäkohtaisia. Näitä ovat kaaviohallitsija (engl.Schema master) sekä toimialueen nimihallitsija (engl. Domain naming master). Metsäkohtaisia rooleja voi olla vain yksi per metsä (ks. kuva 6). (Microsoft 2020a.)



Kuva 6: FSMO-roolien laajuus. (windowstechno)

Toimialueen ohjauskoneista tulisi löytyä ajastettu varmistustyö, jolla voidaan taata Active Directoryn ei-auktoritatiivinen tai auktoritatiivinen palautus. Ei-auktoritatiivinen tarkoittaa, että varmistuksesta voidaan palauttaa yksittäisiä objekteja. Auktoritatiivisessa palautuksessa voidaan palauttaa koko hakemisto. Varmistustyöt tulisi ajoittaa suoritettavaksi tasaisin väliajoin, mielellään päivittäin. Varmistusten sijainti tulisi suunnitella siten, että varmistukset löytyisivät paikalliselta levyltä sekä palvelimen ulkopuolella olevasta tallennussijainnista. Palvelimen ulkopuolisena sijaintina voi toimia esimerkiksi NAS (engl. network attached storage) tai varmistuksiin tarkoitettu pilvipalvelu. Tällä toimenpiteellä voidaan turvata datan palautus myös niissä tilanteissa, joissa palvelimen omat levyt vioittuvat. (netwrix2017d)

Jotta mahdollinen palautus voidaan tehdä, tulee olla tiedossa toimialueen DSRM-salasana (engl. Directory services recovery mode). DSRM on toiminto, jolla toimialueen ohjauskone voidaan ottaa irti verkosta hätähuoltoa tai varmistusten palautusta varten. Mikäli salasana ei ole tiedossa, tulee vaihtaa mahdollisimman pian NTDSUTIL-apuohjelmalla.

Jokaisessa toimialueessa tulisi olla vähintään kaksi toimialueen ohjauskonetta, jotta pienin mahdollinen vikasietoisuus tapahtuisi. Kahden ohjauskoneen vikasietoisuus ei välttämättä riitä varmistamaan kaikkien palveluiden toimivuutta vikatilanteessa. Varmistusten tärkeys ilmenee siinä, että aina ei tarvita fyysistä vikatilannetta, jotta varmistuksia tarvitaan. On tilanteita, jossa Active Directorysta poistetaan objekteja vahingossa tai palveluun tehdään konfiguraatiovirhe. Tällaisissa tilanteissa virhe kopioituu nopeasti kaikille

toimialueen ohjauskoneille. Siksi on tärkeää, että Active Directorystä on olemassa ajantasainen varmuuskopio.

Toimivan varmistusprosessin lisäksi tulee luoda yksityiskohtaiset ohjeet mahdollisen katastrofitilanteen varalle. Lisäksi Active Directoryn osalta tulisi tehdä erillinen kirjallinen katastrofaalisen tilanteen palautusohje (engl. disaster recovery plan), jossa on etukäteen ohjeistettu palauttaminen eri vikatilanteista. Varmistuksien toimivuudesta tulisi varmistua tasaisin väliajoin suorittamalla testipalautuksia siinä määrin kuin ympäristössä on mahdollista aiheuttamatta liiallista haittaa käyttäjille tai palveluille.

Kuten todettu, Active Directory toimii modernin IT-infrastruktuurin selkärankana. Active Directoryn merkittävyyden vuoksi sen palveluiden tarkasteluun tulisi käyttää paljon resursseja ja tarkastelun tulisi näkyä myös raportoinnissa. Teknisen raportoinnin lisäksi tulisi Active Directoryn tärkeydestä koko IT-infrastruktuurille olla oma osionsa. Tässä osiossa selvitetään, miksi Active Directory on tärkeä ja miksi sen ylläpitämiseen ja varmentamiseen tulisi kuluttaa merkittäviä resursseja.

Raportissa tulisi käydä ilmi ainakin seuraavia asioita: 1. kuinka monta metsää ja puuta infrastruktuurissa on 2. kuinka monta toimialuetta infrastruktuurissa on 3. mitkä ovat metsän ja puun toiminnallisuustasot sekä miten toiminnallisuustasoja voisi kehittää 4. kuinka monta ohjauskoneobjektia toimialueella 5. miten FSMO-roolit tulisi jakaa palvelimien kesken ja miksi niiden toiminnan vikasietoisuus on tehtäväkriittistä ympäristölle 6. kuinka palvelinten varmistukset on varmistettu.

4 HIERARKIAT JA KOKOONPANOT

OU-hierarkialla tarkoitetaan Active Directoryn alaosastoa, mihin voidaan asettaan toimialueen käyttäjiä, ryhmiä, tietokoneita ja muita järjestelmällisiä yksiköitä. järjestelmälliset yksiköt voidaan luoda peilaamaan sekä organisaation funktionaalista rakennetta että yritysrakennetta. Näin ollen OU-hierarkiaan ei ole yhtä oikeaa suositeltua rakennetta vaan siinä heijastuu organisaation koko ja kompleksisuus. Pienen organisaation OU-rakenne saattaa olla hyvin yksinkertainen, sillä oikeuksia voidaan pienellä vaivalla hallita helposti. Isommassa organisaatiossa on suositeltavaa luoda kattava OU-rakenne, jotta oikeuksien jakaminen olisi mahdollisimman automatisoitua. (Indianauniversity2019)

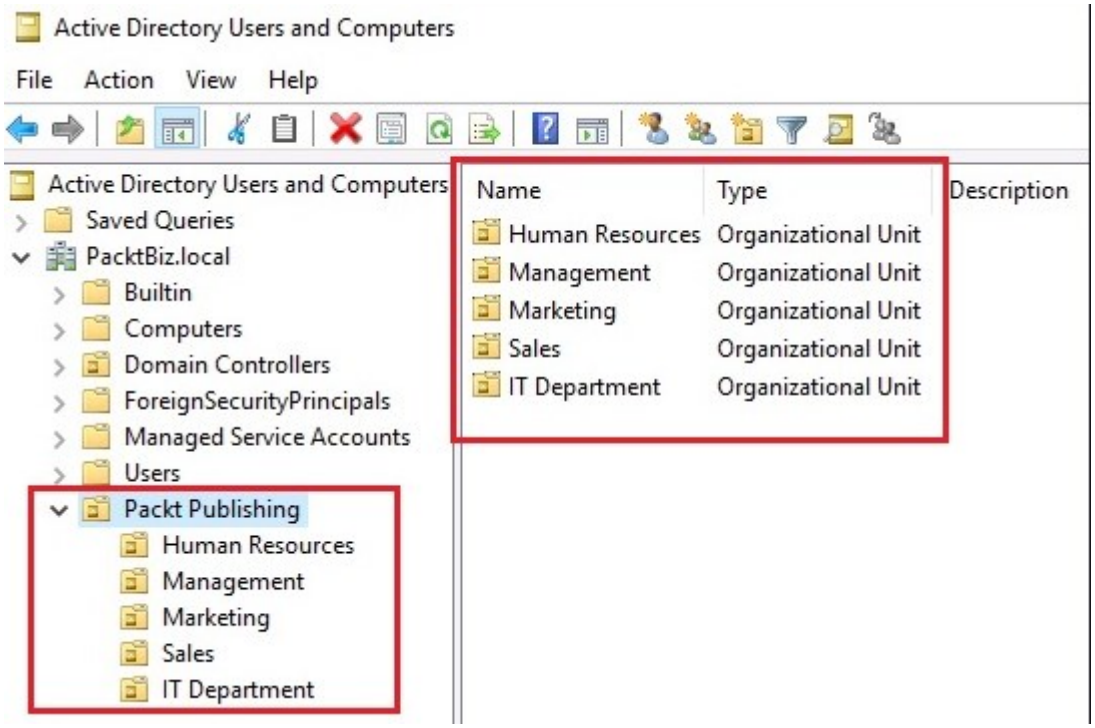
OU:t eli organisaatioyksiköt (engl.organizational unit) ovat säiliöitä, joissa Active Directoryn objekteja säilötään. Niillä on kaksi eri funktiota: visuaalisesti organisoida objekteja ja ryhmittää objekteja. Objektien visuaalinen organisoiminen tekee niistä mahdollisimman ihmisluettavia. Objekteja ryhmitetään, jotta objektiryhmiä vasten voidaan asettaa ryhmäkäytäntöjä (esimerkiksi kirjanpitäjäryhmälle voidaan ryhmäkäytännöllä antaa oikeudet verkkokansioon, jossa säilytetään vain kirjanpitäjille tarkoitettua dataa). Käyttäjien ryhmittäminen mahdollistaa myös hallinnan jakamisen siten, että vain osalla järjestelmänvalvojista on oikeuksia muokata tiettyjä ryhmiä. Esimerkiksi siten, että vain toimialueen järjestelmänvalvojat -ryhmän jäsenillä on oikeus muokata muiden järjestelmänvalvojien objekteja tai luoda niitä. (umich2019)

On suositeltavaa luoda edes jonkinlainen karkea OU-rakenne eikä jättää sitä sellaiseksi, kuin se on ollut Active Directoryn ottaessa käyttöön. Käyttäjätunnusten ja ryhmien osalta harkitaan omien OU:iden rakentamista. Ryhmille tulisi olla oma OU ja käyttäjät, jotka jaetaan esimerkiksi roolituksen tai työpisteen mukaan omaan OU:hun kuten kuvassa 7. Koneobjekteille tulisi luoda myös omat OU:t perustuen työalojen tai toimipisteiden mukaan. Tämä mahdollistaa paremman kohdistuksen tiettyihin työasemiin. On kuitenkin tärkeää, että OU-rakenne olisi sellainen, missä suuret kokonaisuudet olisivat havaittavissa päätasolla. Alitasoja voidaan helposti luoda lisää, joka mahdollistaa enemmän kompleksisuutta.

4.1 Organisaatiollisten yksiköiden suunnittelu

Tehokkaasti hallitussa ympäristössä yksi OU-säiliö, joka edustaa joukkoa koneita tai käyttäjiä, joille halutaan samanlaiset kokoonpanot tai oikeudet. Tämä pitää sisällään asetukset ja esimerkiksi määritykset käyttöoikeuksista Tämä tarkoittaa sitä, että roolituksia ja säiliöitä päästään toteuttamaan vasta kun tiedetään, minkälaisia eri kokoonpanoja halutaan sekä niiden lukumäärä. Organisaatioyksiköiden kattava suunnittelu on yksi tärkeimmistä vaiheista ympäristön hallinnan kannalta.

Organisaation toimintaan ja roolituksiin perustuvaa rakennetta tulisi käyttää pohjana, kun rakennetta suunnitellaan. On tärkeää ymmärtää, mitkä ovat kokonaisuuksia, joita halutaan hallita sekä millainen rakenne palvelee pitkällä aikavälillä parhaiten. Lisäksi maantieteellisyys tulisi ottaa huomioon rakennetta mietittäessä. Usein OU-hierarkia on tyypiltään hybridi. Tällaisissa tapauksissa objektien ryhmittelyn perusteena toimii monia eri muuttujia.



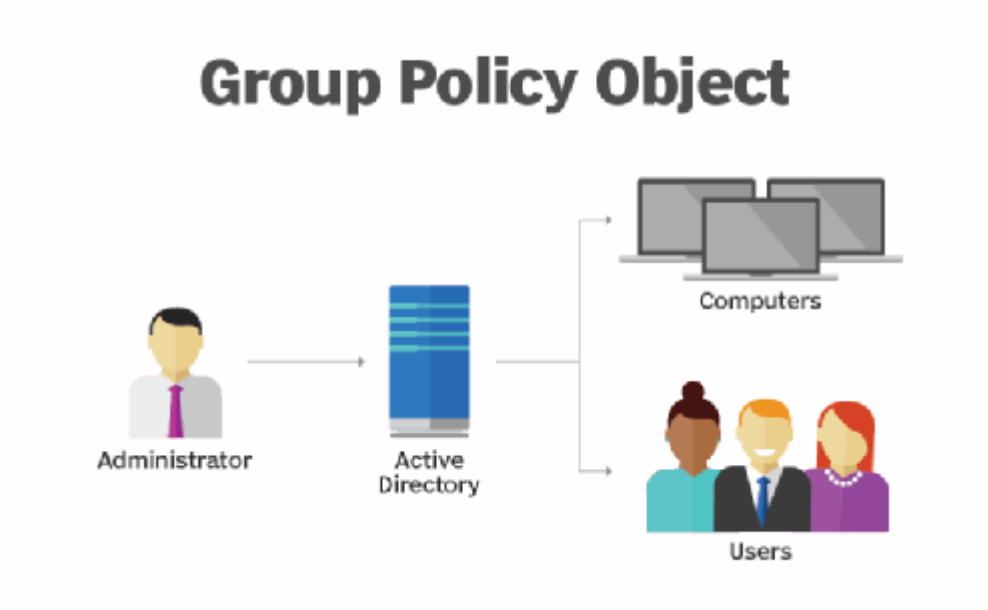
Kuva 7: Active Directoryn OU-rakenne esimerkki. (packtpub)

4.2 Käyttäjä- ja konekokoonpanot

Käyttäjä- ja konekokoonpanot ovat organisaatioyksikköjä, joita vasten on asetettu ryhmäkäytäntöjä. Näitä käytäntöjä voi olla rajaton määrä, mutta niiden toimintaan vaikuttaa vahvasti toimialueen ohjauskoneiden toiminnallisuustasot. Ryhmäkäytännöillä voidaan hallita esimerkiksi Windows 10:n asetuksia ja ominaisuuksia tai tehdä tietyille koneille rekisterimuutoksia.

Käytäntöjä tulisi luoda tietyin käytännöin. Objektien ja asetusten tietoihin tulisi kirjata mitä kyseinen käytäntö tekee ja kuka kyseisen käytännön on luonut. Lisäksi objektista tulisi löytyä muutoshistoriaa ja luonnin päivämäärä. Dokumentointi luo hyvää pohjaa ja auttaa kokonaisuuden hallinnassa ja vianselvityksessä. Ryhmäkäytäntöjen takaisinmallinnus (engl. reverse engineering) on työlästä ja kuluttaa resursseja.

Ryhmäkäytäntöjä tulisi kohdistaa käyttäen organisaatiollista yksikköä tai kokonaisuuksille määriteltyjä ryhmiä. Ryhmäkäytäntöön liittyviä asetuksia ei tarvitse määrittää oletusasetuksista poikkeaviksi, mutta itse objektin oletusasetuksen aktivointi auttaa lukitsemaan asetukset työasemasta käsin. Näin varmistetaan asetusten pysyminen oikeina. Palvelimien kohdalla asetukset, kuten palomuurien asetukset, tulisi aina hallita ryhmäkäytäntöjen kautta. Kuvassa 8 osoitetaan, miten ryhmäkäytäntöjä voidaan asettaa käyttäjä- tai konekohtaisesti.



Kuva 8: Ryhmäkäytäntöjen toiminta ja niiden jakelutavat. (techtarget)

4.3 Ryhmäkäytännöt

Active Directory -ympäristössä keskeisin tavoite kokoonpanojen hallinnassa on sen totuttaminen mahdollisimman tehokkaasti. Tavoite saavutetaan parhaiten niin, että käyttäjä- ja konekokoonpanojen hallinta toteutetaan mahdollisimman kattavasti. Kokoonpanojen hallinta toteutetaan keskitetysti AD:n kautta ryhmäkäytännöillä. (netwrix2017e)

Ryhmäkäytännöt ovat tehokkain ja selkein tapa käyttäjä- ja konetilien hallintaan. Yksinkertaisimmillaan ryhmäkäytännöillä voidaan määrittää käyttäjä esimerkiksi kaikille työasemille, joille hän kirjautuu paikalliseksi järjestelmänvalvojaksi. Ryhmäkäytännöillä voidaan hallita myös sovellusasennuksia ja päivityksiä sekä haluttaessa lisenssejä. Esimerkiksi Microsoft Office 365 tukee Azure Active Directory -synkronisoinnin kautta Office-lisenssien jakelua ryhmäkäytännöillä.

Ryhmäkäytännöt ovat toimialueen järjestelmänvalvojan paras työkalu käyttäjien käyttöoikeuksien ja koneiden hallintaan. Ryhmäkäytännöt voidaan ajaa isojakin organisaatiollisia yksiköitä vasten, jolloin voidaan esimerkiksi määrittää, että tietyn säiliön sisällä oleville käyttäjille annetaan etätyöpöytäyhteys johonkin sovellukseen. Koska organisaation yksikköhierarkia on puumainen, voidaan jokin ryhmäpolitiikka helposti ajaa kaikkia käyttäjiä vasten, jolloin sama käytäntö on kaikilla käyttäjä- tai konekokoonpanoilla käytössä.

4.4 Havainnot

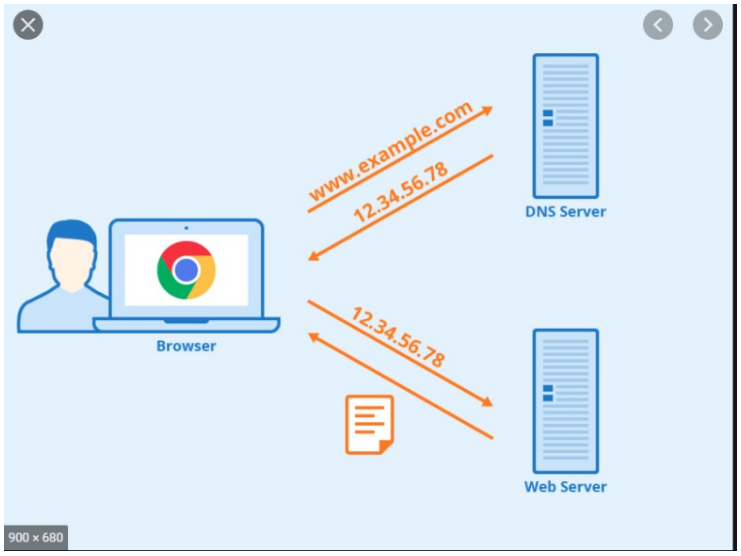
Raportissa tulisi tarkastella sitä, miten Active Directoryn OU-hierarkiaa on kehitetty lähtötilanteesta ja kuinka sitä tulisi kehittää eteenpäin. Organisaatiolliset yksiköt ja ryhmäkäytännöt ovat laitteiden ja käyttäjien hallinnan kannalta järjestelmänvalvojan tärkein ja tehokkain työkalu. Lisäksi tulisi ottaa huomioon, millä tavoin objektit ovat sijoiteltu OU-hierarkiaan ja kuinka ne on nimetty. Esimerkiksi koneobjekteja tulisi nimetä mahdollisimman tehokkaasti ja informatiivisesti juoksevalla luvulla, josta käy ilmi esimerkiksi käyttöjärjestelmäversio, sarjanumero ja työaseman käyttöönottoon viittaava tekijä, kuten vuosi tai kuukausi.

Jos käyttäjäkone ja ryhmäobjektit ovat niiden oletussijainnissa, hallintaa ei voida tehdä kovinkaan tehokkaasti. Active Directoryn hierarkiaa tulisi kehittää alkuperäisestä mallista hallittavampaan ja joustavampaan rakenteeseen. Organisaation toimintaan ja roolituksiin perustuvaa rakennetta olisi hyvä käyttää pohjana, kun rakennetta suunnitellaan. On tärkeää ymmärtää mitkä ovat niitä kokonaisuuksia, joita halutaan hallita ja mikä on rakenne, joka palvelee pitkällä aikavälillä parhaiten myös maantieteellisyyden perusteella.

5 NIMENSELVITYS

DNS eli toimialueen nimijärjestelmä (engl. domain name system) on standardiprotokolla, joka auttaa käyttäjiä löytämään nettisivuja käyttäen ihmisen luettavia osoitteita. Kuten puhelinluettelo, joka auttaa löytämään henkilön numeron etsimällä heidän nimensä, DNS mahdollistaa selaimen osoitekenttään sivun osoitteen kirjoittamalla ohjaamisen vastaavaan IP-osoitteeseen. Ilman DNS:n toimintaa internet sellaisena, kuin me sen tiedämme kaatuisi. Ihmisten ja laitteiden olisi mahdotonta keskustella internet-palvelimien kanssa ihmisluettavien URL:ien avulla (ks. kuva 9).

Toisin kuin puhelinluettelo, DNS-kirjaukset päivittyvät tasaisesti. Tämä tarkoittaa, että palvelimen IP-osoite voi muuttua vaikuttamatta käyttäjiin. Käyttäjät käyttävät aina samaa toimialueosoitetta ja DNS ohjaa käyttäjän selaimen eri osoitteeseen. Kirjauksen päivitys ei kuitenkaan ole välitön, vaan uuden toimialueen rekisteröinnin jälkeen useimmin päivittymiseen menee 12–36 tuntia. Tämän jälkeen maailmanlaajuiset DNS-palvelimet päivittyvät ja kirjaus tulee saataville kaikkialla. (NS1)

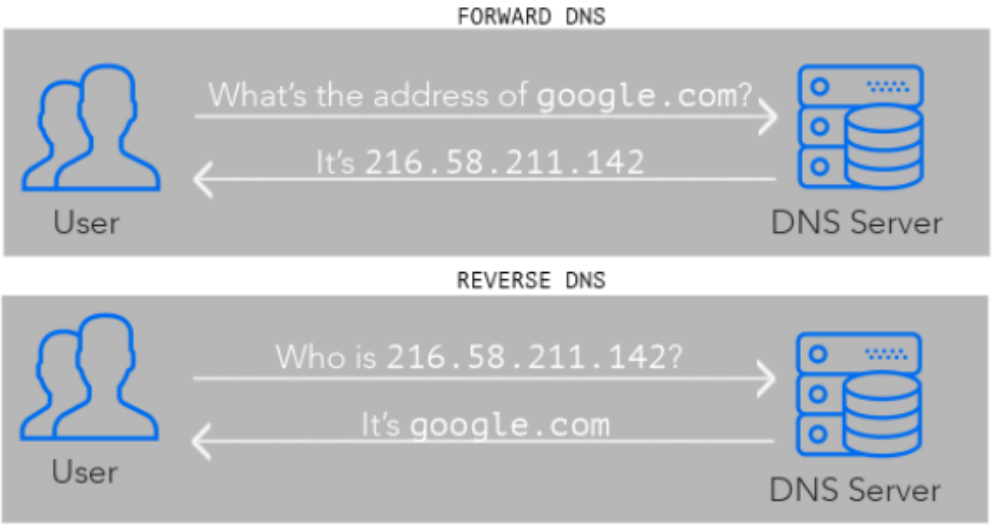


Kuva 9: DNS kysyy IP-osoitetta nettisivulle tai tiedostolle. (seobility)

DNS on AD-ympäristön keskeisin verkkopalvelu, sillä toimialueen ohjauskoneet rekisteröivät palvelunsa DNS-vyöhykkeelle. Eri nimenselvitysmetodeista huolimatta DNS-kyselyt ovat ainoa keino muille palveluille selvittää, mistä AD löytyy. Tämän vuoksi DNS:n lakatessa toimimasta myös AD lakkaa toimimasta. Näiden mukana koko Windows-infrastruktuurin toiminta lakkaa. Hyvänä esimerkkinä tästä toimii toimialueen DNS:ään rekisteröity KDC (engl. Key Distribution Center) -rekisteri. Kaikki Windows-pohjaiset ohjauskoneet, joissa on käynnissä KDC-palvelu, rekisteröivät tämän palvelinkirjauksen. Ilman näitä kirjauksia ei Windows-autentikointi tiedä, mihin Windows-autentikointikyselyt tulee kääntää. Näin ollen esimerkiksi kirjautuminen toimialueelle ei ole mahdollista.

Active Directory-infrastruktuurissa käytetään kahdenlaisia osoitesuunta -tietueita eli itsenäisiä tietokokonaisuuden nimityksiä. Nämä ovat eteenpäin tai väärinpäin kohdennetut tietuet. Eteenpäin kohdennetut hakemistot (engl. reverse lookup zone) toimivat, kuten DNS:n yleisesti odotetaan toimivan. Päätelaite kysyy DNS palvelimelta esimerkiksi: ”Mikä on contoso.com IP-osoite?”, johon DNS-palvelin vastaa, mikäli sen tietueesta löytyy IP-osoite: ”contoso.com IP-osoite on …”. Reverse- ja Forward-lookup zonet havainnollistettuna kuvassa 10.

Lisäksi Active Directoryn DNS-palvelusta löytyy väärinpäin kohdennettu hakemisto (engl. reverse lookup zone). Tässä tietueessa säilytetään tietoja IP-osoitteisiin osoittavista isäntänimistä (engl. hostname). Väärinpäin kohdistetussa tietueessa päätelaite kysyy palvelimelta tiettyä IP-osoitetta vastaavaa isäntänimeä. Nämä tietueet ovat harvemmassa käytössä kuin eteenpäin kohdistetut tietueet, mutta joissain tapauksissa ohjelmisto voi vaatia väärinpäin kohdistetun tietueen käyttämistä. (Servergeeks2014a)

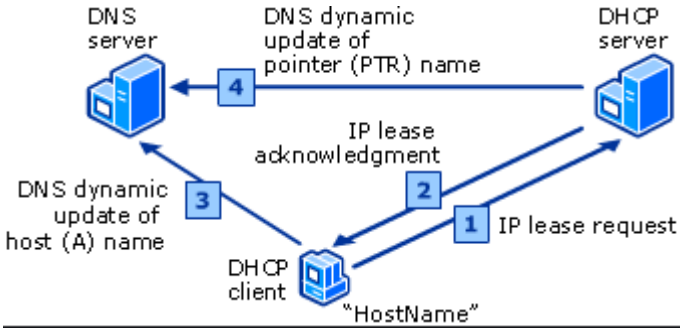


Kuva 10: Forward- ja Reverse DNS-haku. (leadfeeder)

5.1 Toteutus

Toimialueella tulisi olla vähintään kaksi DNS-palvelinta. Yleensä kuitenkin kolme on maksimi, ellei toimialueella ole montaa palvelinfarmia, missä haluttaisiin jakaa DNS-hakujen lastia. Olisi suotavaa, että toinen DNS-palvelin ei olisi paikallinen vaan erillisessä sijainnissa. Tämä auttaa toisen DNS-palvelimen mennessä vikatilaan. (networkworld2003)

DNS voidaan konfiguroida joko täysin käsin tai ottamalla käyttöön dynaamiset päivityksen. Dynaamiset päivitykset mahdollistavat, että DNS-asiakkaat päivittävät ja rekisteröivät resurssitietonsa DNS-palvelimen kanssa, jos muutoksia tapahtuu automaattisesti. Dynaamisissa päivityksissä tulee olla tarkkana, että DNS-palvelussa toimialueen vyöhykkeellä ainoastaan autentikoidut laitteet voitat päivittää tietonsa DNS-vyöhykkeelle (ks. kuva 11). Tämä asetus tulee olla ”Secure only” jollei ”Non-secure” tai ”Secure” asetuksille ole painavaa tarvetta. (Microsoft2013)



Kuva 11: DNS dynaaminen päivitys ja miten se toimii. (technet)

Dynaamisten tietueiden haasteena on, että vyöhykkeille voi jäädä niin sanottuja ei-relevantteja tietueita laitteiden IP-osoitteiden muutosten myötä. Ei-relevantit tietueet voivat aiheuttaa yhteysongelmia, joten niistä tulee päästä eroon. Tämä ongelma voidaan välttää ottamalla käyttöön tietueiden huuhteluasetukset. DNS-huuhteluasetukset tulee ajoittaa siten, että väljähtäneet tietueet tyhjennetään vähintään yhtä usein kuin DHCP-lainat. Hyvä muistisääntö on: olkoon DHCP-laina-aika (eng.DHCP-lease-period) = n päivää. Tällöin huuhteluaikataulutus tulisi olla n-1 päivää. (activeDirectorypro2019)

5.2 Nimenselvityksen raportointi

Nimenselvitys on yksi kriittisimmistä Active Directory:n palveluista, joten on luonnollista, että nimenselvityspalveluun perehdytään syvällisesti. Koska ratkaisut ovat jokaisessa organisaatiossa erilaisia, ei ole yhtä oikeaa pohjaa tai rakennetta palvelun raportointiin. Jotkin asiat ovat kuitenkin universaaleja ja nämä tulisi selvittää ja ilmoittaa raportissa:

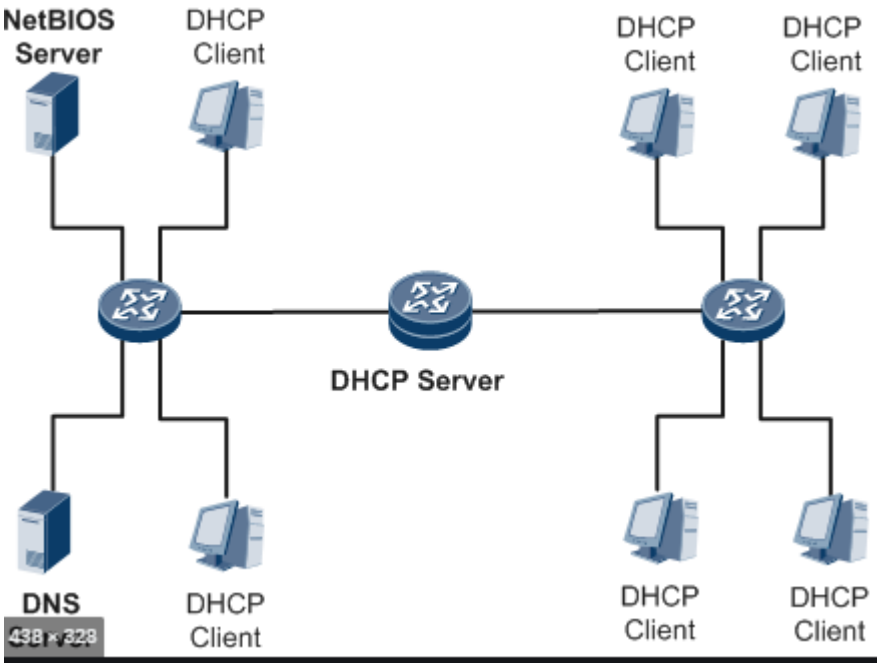
1. Montako nimipalvelinta toimialueella on käytössä?
2. Onko nimipalvelut sijoitettu toimialueen ohjauskoneille vai onko noudatettu hyviä toimintatapoja ja irtautettu nimipalvelut ohjauskoneista?
3. Ovatko dynaamiset nimipäivitykset käytössä? Mikäli ovat, onko ”Secure only”-asetus otettu käyttöön?
4. Huuhdellaanko turhia osoitteita tasaisin väliajoin, ja onko huuhteluissa huomioitu DHCP laina-ajat?

6 IP-OSOITTEET, OSOITEJAKELU (DHCP)

6.1 DHCP ja sen totetutus

DHCP (engl. Dynamic Host Configuration Protocol) on yleinen verkkoprotokolla, jolla jaetaan IP-osoitteita lähiverkkoon kytketyille laitteille, kuten kuvassa 12. DHCP:llä voidaan jakaa lähiverkon laitteille IP-osoitteita kahdella eri tavalla. Dynaamisesti jakamalla, jolloin laite pyytää DHCP-palvelimelta osoitetta ja palvelin vastaa osoitteella, joka on määritetyn osoiteavaruuden sisäpuolella ja vapaana. Vaihtoehtoisesti laitteille voidaan määritellä staattinen osoite, jolloin laitteen verkkokortin MAC-osoite ankkuroidaan tiettyyn IP-osoitteeseen ja sitä ei voida dynaamisesti jakaa sen jälkeen. Millään muulla laitteella samassa lähiverkossa ei siis voi olla samaa osoitetta, joka on varattu staattisena osoitteena toiselle laitteelle.

DHCP-palvelimen välityksellä voidaan jakaa myös muita verkkoasetuksia kuin IP-osoite, kuten oletusyhdyskäytävän tai nimipalvelimien IP-osoitteet. Käytännössä kuitenkin DHCP:n avulla voidaan jakaa lähes mitä vain asetuksia. Yleisimpiä näistä ovat esimerkiksi NTP tai Windowsin SMB-tiedostojaon asetukset.



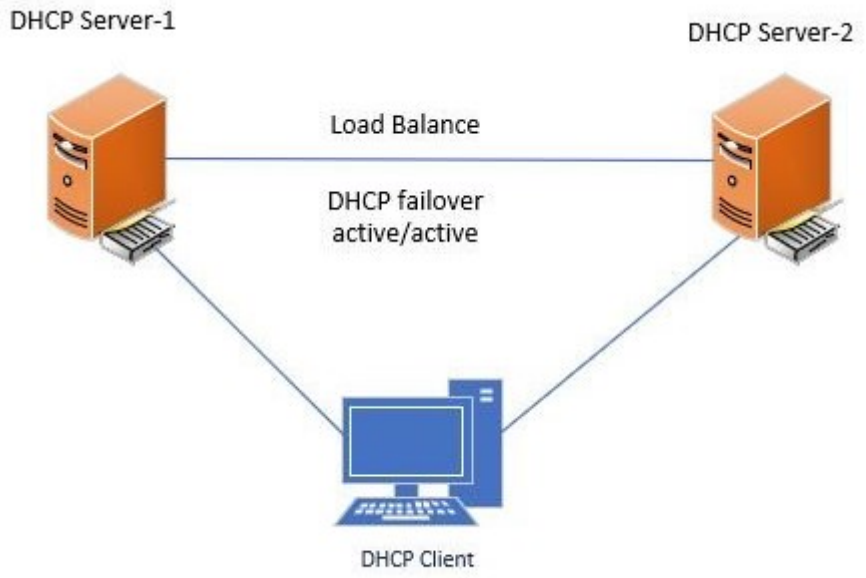
Kuva 12: Kuinka DHCP jakelee osoitteita laitteille. (Huawei)

DHCP voidaan implementoida lukuisilla eri tavoilla, mutta tässä työssä keskitytään Windows-infrastruktuurin Windows-serverin DHCP-palveluun. DHCP ei ole poikkeus ja siinä tulisi toteutua vikasietoisuus. On suositeltavaa, että toimialueella olisi vähintään kaksi palvelinta, joissa on DHCP-palvelu. DHCP-palvelu tulisi olla omalla määritetyllä palvelimellaan eikä esimerkiksi toimialueen ohjauskoneella. (ActiveDirectorypro2020b)

On kaksi suositeltua tapaa konfiguroida Windows-palvelimen DHCP-palveluun. Ensimmäinen on Microsoftin oma DHCP-vikasietoisuuden toiminnallisuus (engl. DHCP failover). Toinen tapa on DHCP-laajuuden jako. Microsoftin omassa vikasietoisuuden toiminnallisuudessa laajuusmääritykset (engl. scope) kopioituvat kaikkien toimialueen DHCP-palvelinten kesken. Määritellään erikseen, mitkä palvelimet toimivat aktiivisena ja mitkä passiivisena. Passiiviset palvelimet muuttuisivat aktiivisiksi, mikäli ensisijainen DHCP-palvelin menisi vikatilaan. (netwrix2017f)

Vaihtoehtoisesti DHCP-palvelu voidaan rakentaa DHCP-laajuuden jaolla. Tässä tapauksessa osoiteavaruus jaetaan usean palvelun kesken. Tässä konfiguraatiossa osoiteavaruus voidaan jakaa esimerkiksi 80/20-jaolla. Toinen palvelin vastaisi 80 %:sta määritellystä osoiteavaruudesta ja toinen 20 %:sta. Etuna tässä toimintamallissa on, että 80 %:n määritellystä osoiteavaruudesta pitäisi riittää jokapäiväiseen toimintaan. Lisäksi koska DHCP-laina-ajat ovat yleensä useita päiviä, vaikka DHCP-palvelin olisi pois käytöstä, on epätodennäköistä, että yli 20 % laitteista tarvitsisi uuden osoitteen tällä välin. DHCP:n jaolla ei kuitenkaan saavuteta yhtä helposti niin hyvää vikasietoisuutta, mitä aktiivi-passiivi-ratkaisussa saavutetaan. (Serverfault)

Microsoftin DHCP-vikasietoisuuden toiminallisuuteen voidaan konfiguroida kuormajako, kuten kuvassa 13. Toista palvelinta ei laiteta odottamaan toisen palvelimen vikatilaa, vaan DHCP:n kuorma jaetaan halutuin prosentein molempien palvelinten kesken. Yleinen toimintatapa kahden DHCP-palvelimen kanssa on jakaa kuorma 50/50. Tällä toteutustavalla ei yhtä palvelinta kuormiteta liikaa, ja mikäli palvelimet ovat teholtaan vastaavia pitäisi toisen palvelimen ollessa vikatilassa toisen kyetä hoitamaan koko kuorma, kunnes toinen palvelin saadaan taas toimintaan. Tämä tapa on yleinen ja suositeltava tapa hoitaa vikasietoinen DHCP-palvelu.



Kuva 13: DHCP:n kuormanjako ja vikasietoisuus. (activeDirectorypro2020a)

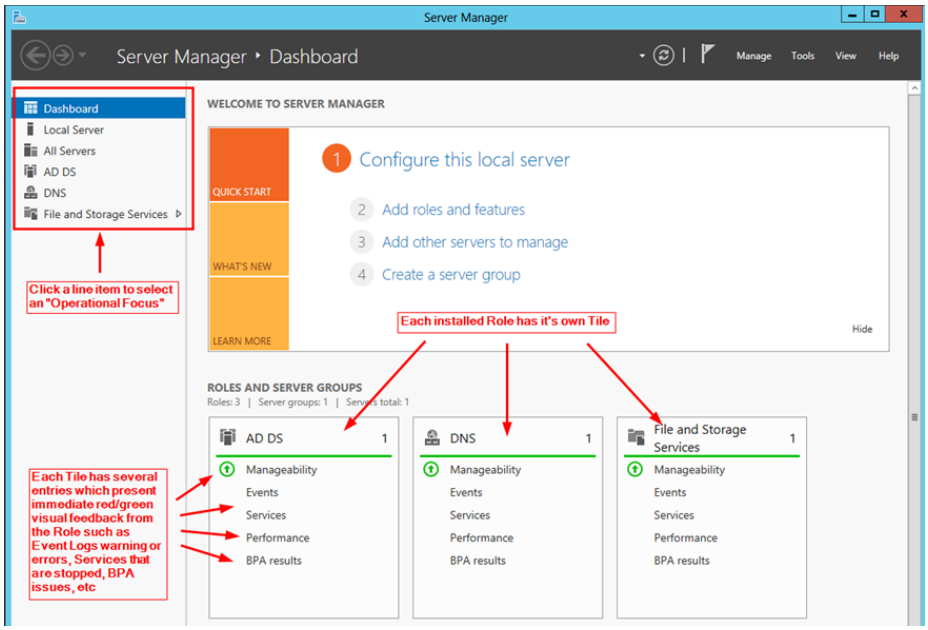
6.2 Raportointi

DHCP:n raportoinnissa on äärimmäisen tärkeää, että auditoija painottaa DHCP:n kriittisyyttä infrastruktuurille ja sen toiminnalle. DHCP vastaa kaikista IP-osoitteista, joita toimialueella on käytössä, ei yksikään verkkolaite toimi DHCP:n vikatilassa. Tulisikin raportissa vahvasti keskittyä osoitejakelun vikasietoisuuteen, sekä palveluiden sijainteihin. Vikasietoisen ympäristön DHCP palveluiden konfiguraatiot on tärkeä tarkistaa osoiteavaruuksien päällekkäisyyksien varalta.

7 TEKNINEN TOTEUTUS

7.1 Active Directory

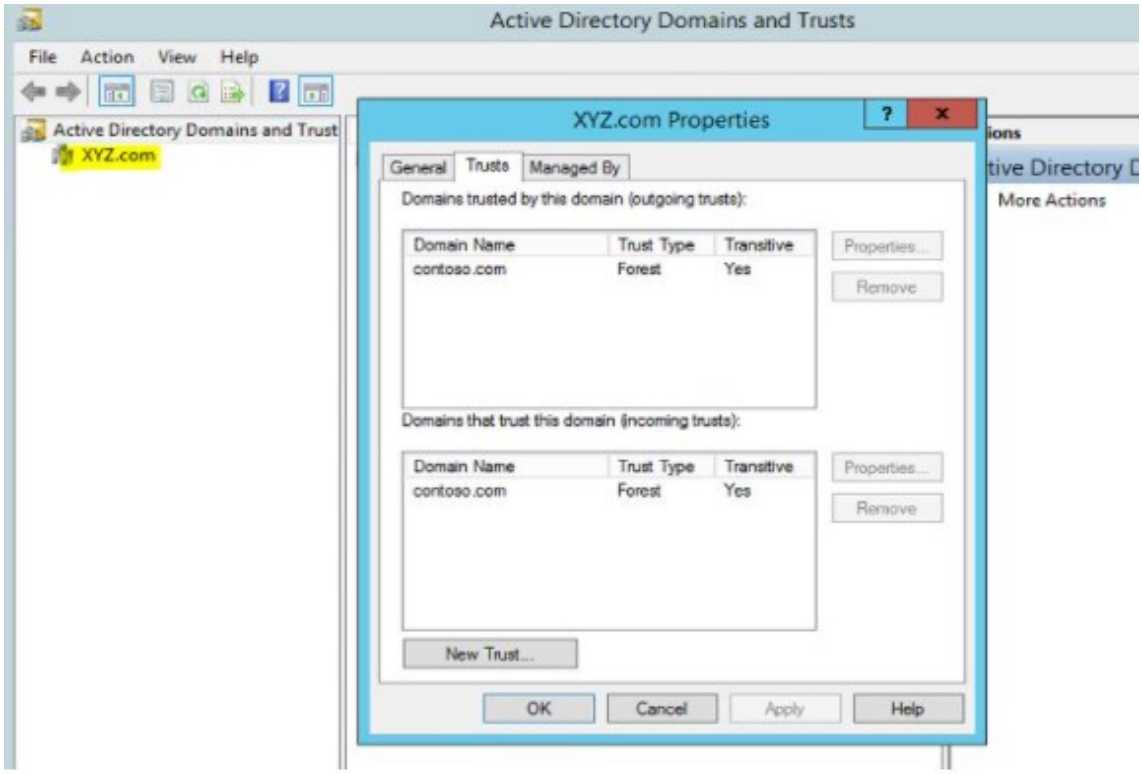
Toimialueen Windows-palvelimille asennettujen roolien ja palvelujen tutkiminen kannattaa aloittaa jokaisella Windows-palvelimella olevalla palvelimen hallinta -käyttöliittymällä (engl. server manager). Palvelimen hallinta listaa kaikki ohjauskoneelle määritellyt roolit ja palvelut (ks. kuva 14). Kuten ylempänä mainitsin, jos palvelin on määritelty toimialueen ohjauskoneeksi, sillä tulisi olla mahdollisimman vähän muita palveluita ja rooleja.



Kuva 14: Palvelimen hallinta -käyttöliittymä (Microsoft2012)

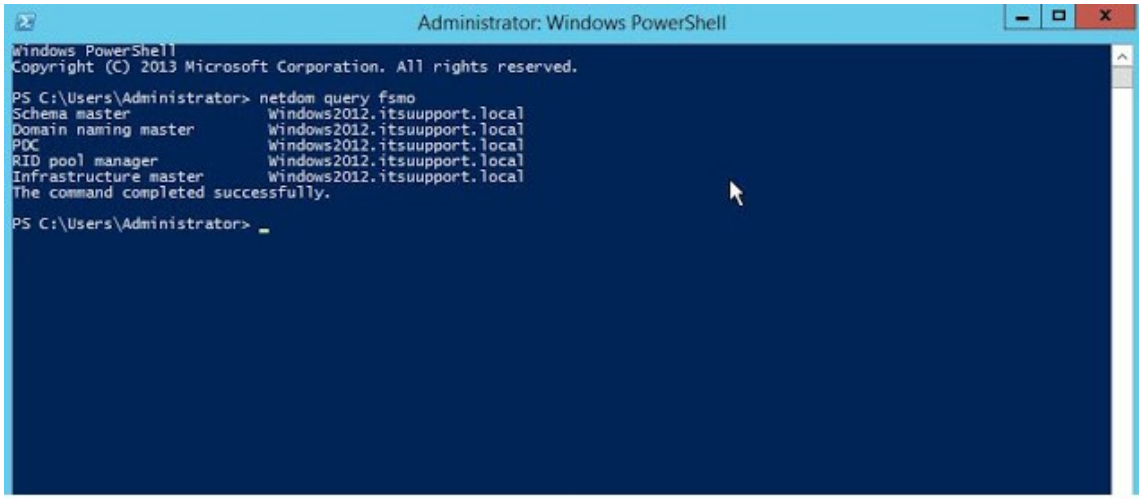
Active Directory toimialueille ja luottamussuhteille (engl. Active Directory Domains and Trusts, AD DS) -käyttöliittymästä, nähdään palvelimelle konfiguroitu toimialue ja metsä, johon se on liitetty. AD DS -käyttöliittymästä voidaan myös tarkastella, onko toimialueesta tehty luottamussuhteita muihin toimialueisiin. Lisäksi metsän ohjauskoneelta voidaan tutkia, onko metsällä luottamussuhdetta toiseen metsään. AD DS -käyttöliittymästä

voidaan tutkia toimialueen sekä metsän toiminnalliset tasot (ks. Kuva 15).



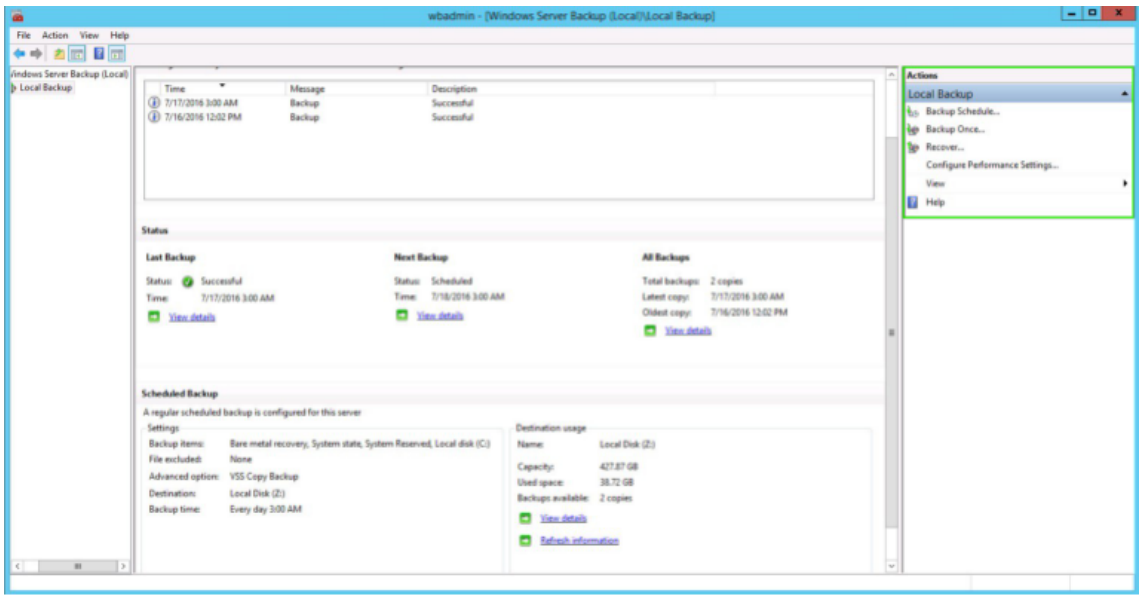
Kuva 15: Toimialueen ja metsän luottamussuhteiden tarkistaminen (Rebeladmin2015)

FSMO-roolien sijainnin tarkistaminen onnistuu helpoiten ohjauskoneen korotetun oikeuden PowerShell-komennolla **”netdom query fsmo”**. Komento listaa FSMO-roolin sekä palvelimen, jolle rooli on konfiguroitu (ks. kuva 16). Listaa tulkitsemalla voidaan selvittää, millaista FSMO-roolien mallia toimialueella käytetään.



Kuva 16: FSMO-roolien sijaintien tarkistaminen (Itsupport2019)

Varmistusten tekninen toteutus vaikuttaa siihen, miten niiden toteutuma voidaan todentaa. Tässä työssä keskityn kuitenkin vahvasti Microsoftin omien tuotteiden tulkitsemiseen. Windowsin oma Windows Server Backup -käyttöliittymä kertoo varmistusten tämänhetkisen tilan selkeästi. Käyttöliittymässä on tiedote siitä, milloin jotain on tapahtunut, mitä on tapahtunut sekä onko tapahtuma onnistunut (ks. kuva 17). Lisäksi käyttöliittymästä voidaan tarkastella, kuinka usein varmistukset ajetaan ja mikä on varmistusten sijainti.



Kuva 17: Windows-palvelimen varmennuksienhallinta (Hostgator)

7.2 Kokoonpanot ja OU-hierarkia

Active Directory käyttäjille ja tietokoneille (engl. Active Directory Users and Computers, ADUC) on toimialueen ohjauskoneen toiminnallisuus, joka mahdollistaa OU-hierarkian muokkaamisen ja objektien sen sisään luomisen. ADUC mahdollistaa OU-hierarkian visuaalisen tutkimisen ja sen sisällä olevien objektien tarkistamisen (ks. Kuva 7). Yksinään OU-hierarkian tutkiminen on vain visuaalinen varmistus siitä, onko hierarkialle tehty joitain roolin asennuksen jälkeen.

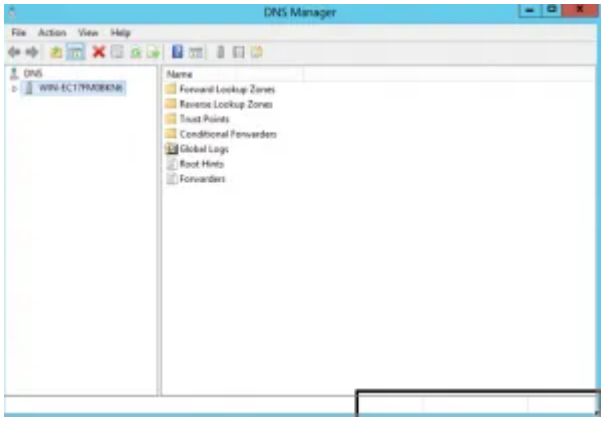
ADUC:in sisään sijoitetuilla ryhmäobjekteilla voidaan automatisoida käyttäjä- ja oikeushallintaa ja onkin siis tärkeää myös tutkia, kuinka paljon näitä on käytössä. Ryhmäobjektien määrä saadaan PowerShell komennolla **“Get-ADGroup -Filter * | measure-object”.** Itsessään määrä ei vielä kerro, kuinka paljon ryhmäobjekteista on ajossa, mutta siitä nähdään, hyödynnetäänkö ryhmäobjekteja käyttäjä- ja oikeushallinnassa.

Ryhmäkäytäntöjä tutkiessa voidaan helposti tarkistaa luotujen ryhmäkäytäntöjen määrä PowerShell komennolla **” (get.gpo -all).count”**. Ryhmäkäytäntöjen läpikäyminen ei ole merkityksellistä auditoinnin kannalta. Auditoinnin näkökulmasta on tärkeämpää vain tutkia, käytetäänkö saatavilla olevia resursseja mahdollisimman tehokkaasti. Ryhmäkäytännöistä tulisi kuitenkin tarkistaa, että ryhmäkäytännöillä vaaditaan salasanan vaihtamista riittävän usein. Salasanojen tulisi myös noudattaa riittävää monimutkaisuustasoa.

Toimialueen hallintatunnuksia tulisi olla mahdollisimman vähän, ja niitä tulisi käyttää vain silloin kuin niitä tarvitaan. Tuleekin tarkistaa hallintatunnusten määrä PowerShell komennolla **“(Get-ADGroupMember -Identity “Domain Admins”).count”**. Poistamalla sulkeet ja **”. count”** -muuttuja, saadaan lista kaikista toimialueen hallintatunnus -tasoisista tunnuksista. Hallintatunnusten määrä tulisi minimoida ja ylimääräiset poistaa käytöstä. Hallintatunnuksen salasanan ei tulisi olla ”never expire” -tilassa. Tunnukset joiden salasana on vanhenematon saadaan komennolla **”get-aduser -filter -properties Name, PasswordNeverExpires : where {$_.passwordNeverExpires -eq ”true”} : where {$_.enabled -eq ”true”} : Format-Table -Property Name, PasswordNeverExpires -AutoSize”**. Komennon tuottamaa listaa tuleekin verrata hallintatunnusten listaan ja varmistaa ettei listalla ole päällekkäisyyksiä.

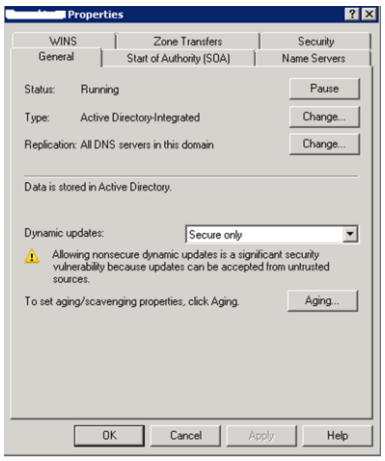
7.3 Nimenselvitys ja DHCP

Palvelimella, jossa nimenselvitys on konfiguroituna roolina, voidaan avata DNS hallinta -käyttöliittymä. Käyttöliittymästä nähdään toimialueen kaikki palvelimet, jossa on DNS-rooli (ks. kuva 18). Käyttöliittymästä voidaan tarkistaa konfiguroidut eteen- ja taaksepäin kohdennetut hakemistot. Hakemistoista tulee tarkistaa, ettei konfiguroituna ole käytöstä poistuneita palvelimia tai osoiteavaruuksia.

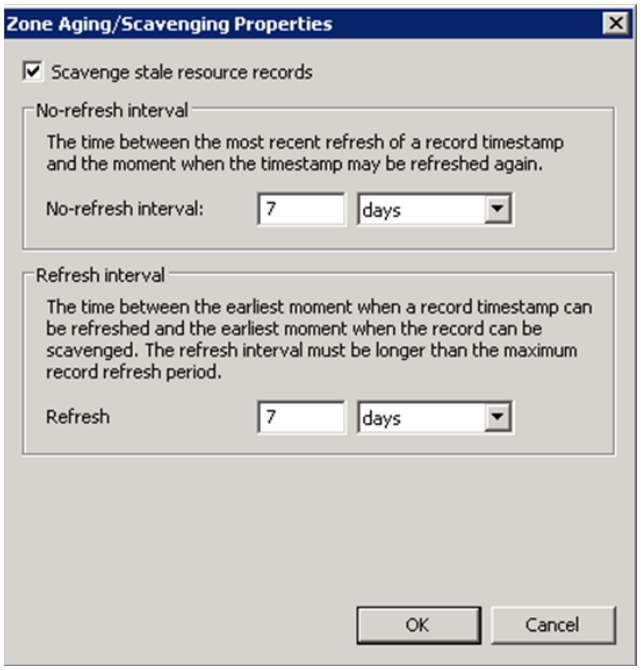


Kuva 18: Nimenselvityksen käyttöliittymä (Krypted2013)

Eteenpäin kohdennetuista hakemistoista voidaan tarkistaa oman toimialueen lisäasetusten alta, yleiset-välilehden alta, dynaamisten päivitysten tila. Dynaamisten päivitysten tulisi olla ”secure only” -tilassa (ks. kuva 19). Yleiset-välilehden ”aging”-lisävalikon alta voidaan tarkistaa, onko vyöhykkeiden huuhtelu käytössä, ja kuinka usein huuhtelu tapahtuu (ks. kuva 20).

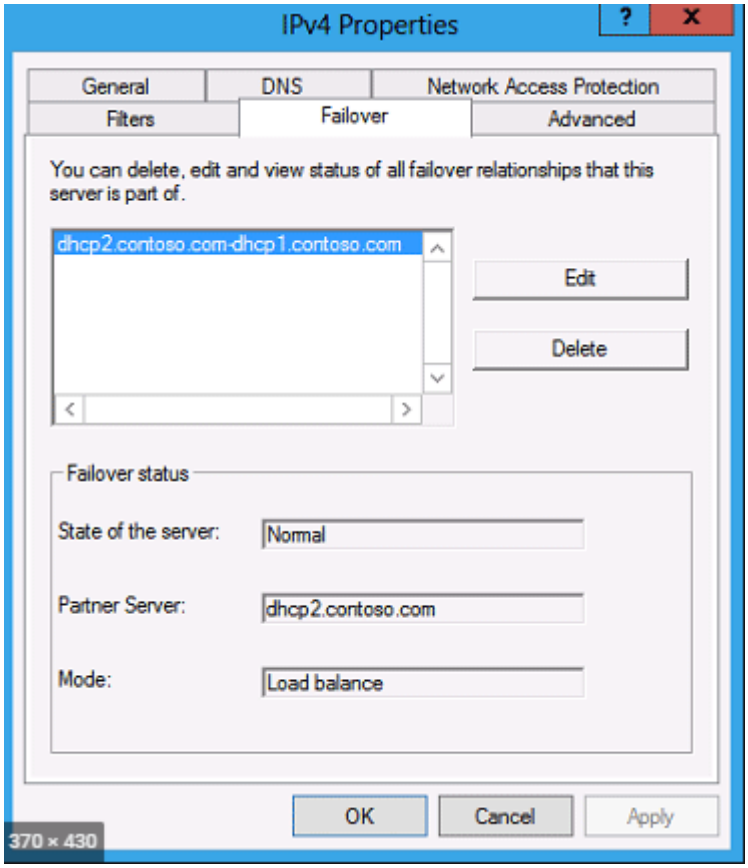


Kuva 19: Nimenselvityksen dynaamisten päivitysten tila. (Microsoft2014a)



Kuva 20: Nimenselvityksen huuhteluiden konfiguraatio. (Microsoft2014b)

Palvelimilta, joissa on asennettuna DHCP-rooli, voidaan tutkia DHCP-asetuksia DHCP-käyttöliittymän avulla. Käyttöliittymässä on listattuna kaikki DHCP-roolin omaavat palvelimet, sekä niille konfiguroidut asetukset. Palvelinten alta löytyvän IPv4 hakemiston lisäasetuksista voidaan tarkastella konfiguroitua tilaa (ks. kuva 21). Vikasietoisuus-välilehdestä nähdään tila, mikä palvelimelle on konfiguroitu. Tila voi olla aktiivipassiivi-tila tai suositellumpi kuormanjakotila. Lisäksi muokkaa-lisävalikon alta voidaan tarkastella kuormanjakotilassa olevien palvelimien kuormanjaon suhdetta.



Kuva 21: DHCP:n viansietoisuuden tila. (Microsoft2016)

8 LOPUKSI

Auditoinnin tavoitteena on varmistaa, että organisaation IT-infrastruktuuri toimii parhaalla mahdollisella tavalla juuri auditoitavan organisaation tarpeiden mukaan. Infrastruktuurintoiminnan tulisi olla samaan aikaan sekä mahdollistavaa että toteuttavaa. Infrastruktuurin tulisi myös olla mahdollisimman helppo ylläpitää, jotta se mahdollistaa resurssien hyödyntämisen parhaalla mahdollisella tavalla.

Auditoinnin tarkoituksena on varmistaa, että yllä mainitut asiat toteutuvat. Infrastruktuurin tekninen auditointi pyrkii selvittämään IT-infrastruktuurin nykytilan ja varmistamaan, että organisaatiossa noudatetaan palvelujen ja toimintojen parhaita toimintamalleja. Turvallinen ja toimiva infrastruktuuri mahdollistaa infrastruktuurin resurssien hyötyjen maksimoinnin samalla vähentäen ylläpitokustannuksia.

IT-infrastruktuurin auditointiin tutustuminen on osoittanut, miten merkittävä osa organisaation infrastruktuurin toiminnan turvaamista auditointi on. Auditoinnin päätteeksi luovutettava raportti on tärkeä osa prosessia, sillä raportin on tarkoitus antaa todenmukainen kuva IT-infrastruktuurin nykytilasta.

Raportti tulee kirjoittaa siten, että myös teknisesti kouluttamaton henkilö kykenee ymmärtämään sen sisällön. Tämä takaa, että organisaation kaikille osapuolille jää tarkka käsitys IT-infrastruktuurin sen hetkisestä toiminnasta. Koska toimiva IT-infrastruktuuri takaa organisaation turvallisen toiminnan, on kiinnitettävä huomiota infrastruktuurin jatkuvaan ylläpitoon ja kehitykseen.

Auditointi perustuu vahvasti auditoijan henkilökohtaiseen kokemukseen ja osaamiseen. Auditoija tekee auditoinnin pääasiassa manuaalisesti ja auditoinnissa toistuvat samat työvaiheet. Kuitenkin koska jokaisen organisaation IT-infrastruktuuri on ainutlaatuinen, on myös jokainen auditointi sisällöltään erilainen. Jokaisen organisaation tarpeiden ollessa erilaisia tulee auditoijalla olla selkeä kuva organisaation toiminnasta. Jotta auditoija voi antaa organisaatiolle räätälöityjä kehitysehdotuksia, tulee auditoijan ymmärtää organisaation toiminnan tärkeimmät osa-alueet.

Erilaisia sertifikaatteja ja luokituksia on useita. Auditoinnille on haastavaa luoda tiettyä toimintamallia, sillä jokainen organisaatio ja sen toimintamallit ovat erilaisia. IT-infrastruktuurin auditointiperiaatteisiin tutustuminen on osoittanut, että sekä organisaatiot että auditoijat hyötyisivät standardoidusta auditointiprosessista. Esimerkiksi auditointiin liittyvien

sertifikaattien tai luokitusten avulla voitaisiin osoittaa auditoijan pätevyys paremmin. Standardien avulla voitaisiin paremmin selvittää, mitä auditoijalta ja auditoinnilta odotetaan. Kun organisaation odotukset ja auditoijan pätevyys kohtaavat, päästään lähemmäs organisaation toimintaa tukevaa IT-infrastruktuuria.

LÄHTEET

ActiveDirectorypro 2019. How to Configure DNS Aging and Scavenging (Cleanup Stale DNS Records). Viitattu 5.4.2021 https://activeDirectorypro.com/how-to-configure-dns-aging-and-scavenging/

activeDirectorypro2020a. Top 16 DHCP Best Practices: The Ultimate Guide. Viitattu 25.4.2021 https://activeDirectorypro.com/dhcp-best-practices/

ActiveDirectoryro2020b. Don't Put DHCP on Your Domain Controller. Viitattu 5.4.2021 https://activeDirectorypro.com/dhcp-best-practices/#dhcp-on-domain-controller

askme4tech 2019. Viitattu 25.4.2021 https://askme4tech.com/how-use-hyper-v-best-practices-analyzer-windows-server-2016

Hostgator. Windows Server Backup. Viitattu 13.5.2021 https://www.hostgator.com/help/article/windows-server-backup

Huawei https://support.huawei.com/enterprise/en/doc/EDOC1100146985/24a20adf/configuring-a-dhcp-server

indianauniversity 2019. About organizational units in Active Directory. Viitattu 2.4.2021 https://kb.iu.edu/d/atvu/

Itsupport2019, Vihaan. How to check FSMO Roles holder in Active directory. Viitattu 13.5.2021 https://www.itsuupport.com/2019/03/how-to-know-who-is-fsmo-role-holders-in.html

Krypted2013. Managing DNS In Windows Server 2012. Viitattu 13.5.2021 https://krypted.com/windows-server/managing-dns-in-windows-server-2012/

leadfeeder, Anna Crowe 2021. Viitattu 26.4.2021 https://www.leadfeeder.com/blog/what-is-reverse-dns-and-why-you-should-care/

Microsoft 2012a. Managing Operations Master Roles. Viitattu 29.3.21 https://technet.microsoft.com/en-us/library/cc816945(ws.10).aspx

Microsoft 2020a. FSMO placement and optimization on Active Directory domain controllers. Viitattu 28.3.2021 https://support.microsoft.com/en-us/help/223346/fsmo-placement-and-optimization-on-active-Directory-domain-controllers

Microsoft2013. DNS "Dynamic Updates" - Secure only vs Nonsecure and secure. Viitattu 5.4.2021 https://social.technet.microsoft.com/Forums/windows/en-US/68be2d67-

25d9-4e72-b827-2d6f3b23bf76/dns-quotdynamic-updatesquot-secure-only-vs-nonsecure-and-secure?forum=winserverNIS

Microsoft2012, Michael Hildebrand. Welcome to Server Manager...2012-style. Viitattu 13.5.2021 https://techcommunity.microsoft.com/t5/core-infrastructure-and-security/welcome-to-server-manager-2012-style/ba-p/255712

Microsoft2014a. How DNS Aging and Scavenging Works. Viitattu 13.5.2021 https://social.technet.microsoft.com/wiki/contents/articles/21724.how-dns-aging-and-scavenging-works.aspx

Microsoft2014b. How DNS Aging and Scavenging Works. Viitattu 13.5.2021 https://social.technet.microsoft.com/wiki/contents/articles/21724.how-dns-aging-and-scavenging-works.aspx

Microsoft2016. Step-by-Step: Configure DHCP for Failover. Viitattu 13.52021 https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2012-r2-and-2012/hh831385(v=ws.11)

networkword2003. How many DNS servers do I need? Viitattu 5.4.2021 https://www.networkworld.com/article/2335470/how-many-dns-servers-do-i-need-.html

Netwrix2017a, Brian Svidergol. Forests in Active Directory. Viitattu 29.3.2021. https://blog.netwrix.com/2017/01/30/forests-in-active-Directory/

Netwrix2017b, Brian Svidergol. What Are the 5 FSMO Roles in Active Directory. Viitattu 29.3.2021 https://blog.netwrix.com/2017/01/31/what-are-the-5-fsmo-roles-in-active-Directory/

Netwrix2017c, Jeff Melnick. What are Group Policy and Group Policy Objects? Viitattu 29.3 https://blog.netwrix.com/2017/02/17/group-policy/ GPO

Netwrix2017d, Brian Svidergol. Active Directory Replication Viitattu 29.3.2021 https://blog.netwrix.com/2017/02/20/active-Directory-replication/

Netwrix2017e, Jeff Melnick. What are Group Policy and Group Policy Objects? Viitattu 29.3 https://blog.netwrix.com/2017/02/17/dns-in-active-Directory/

Netwrix2017f, Brian Svidergol. Dynamic Host Configuration Protocol (DHCP) Viitattu 13.4.2021 https://blog.netwrix.com/2017/02/17/dynamic-host-configuration-protocol-dhcp/ DHCP conf

NS1. What is DNS? DNS Explained. Viitattu 28.3.2021 https://ns1.com/resources/what-is-dns

packtpub. Understanding organizational units (OUs) and containers. Viitattu 22.4.2021 https://subscription.packtpub.com/book/virtualization_and_cloud/9781788626569/4/ch04lvl1sec23/understanding-organizational-units-ous-and-containers-3-2

Rebeladmin2015, Dishan M. Francis. Configuring Trusts – Part 4. Viitattu 13.5.2021 https://www.rebeladmin.com/2015/02/configuring-trusts-part-4/

seobility. DNS Server. Viitattu 30.4.2021 https://www.seobility.net/en/wiki/DNS_Server

Serverfault 2012. Can I have multiple DHCP servers on one network? Viitattu 5.4.2021 https://serverfault.com/questions/368512/can-i-have-multiple-dhcp-servers-on-one-network

Servergeeks2014. Dependency of Active Directory on DNS. Viitattu 28.3.21. https://servergeeks.wordpress.com/2014/05/12/dependency-of-active-Directory-on-dns/

technet, MF47 2017. Viitattu 8.5.2021 https://social.technet.microsoft.com/Forums/ie/en-US/778c7f0f-6f7a-4da3-94b8-8b54f51c116e/dns-dynamic-updates-for-non-domain-computers?forum=winserver8gen

techtarget,Linda Rosencrance, Amy Kucharik 2019. Viitattu 8.5.2021 https://searchwindowsserver.techtarget.com/definition/Group-Policy-Object

umich2019. Active Directory Users, Groups, and OUs. Viitattu 2.4.2021 https://documentation.its.umich.edu/node/944

Varonis, Jeff Petters 2020. What is an Active Directory Forest? Viitattu 3.5.2021 https://www.varonis.com/blog/active-Directory-forest/

windowstechno, Vipan Kumar 2018. How to Quickly check FSMO roles. Viitattu 3.5 https://www.windowstechno.com/how-to-quickly-check-fsmo-roles-method-2/

Youtube, itfreetraining, 2012. MCITP 70-640: Active Directory Forest Functional Levels. Viitattu 8.5.2021 https://www.youtube.com/watch?v=q02SEygch1M