TAMPEREEN
AMMATTIKORKEAKOULU

LIIKETALOUS

TUTKINTOTYÖRAPORTTI

Active Directoryn katastrofitilanteesta toipuminen

Kai Stenvik

Tietojenkäsittelyn koulutusohjelma
syyskuu 2005
Työn ohjaaja: Harri Hakonen

TAMPERE 2005

TAMPEREEN
AMMATTIKORKEAKOULU

LIIKETALOUS

Tekijä(t):	Kai Stenvik
Koulutusohjelma(t):	Tietojenkäsittelyn koulutusohjelma
Tutkintotyön nimi:	Active Directoryn katastrofitilanteesta toipuminen
Title in English:	Active Directory Disaster Recovery
Työn valmistumis-kuukausi ja -vuosi:	Syyskuu 2005
Työn ohjaaja:	Harri Hakonen

Sivumäärä: 60

TIIVISTELMÄ

Tutkintotyöni käsittelee Windows Active Directory -palvelun katastrofitilanteesta toipumista. Windows-pohjaisissa työasemaympäristöissä on laajalti käytössä Active Directory -palvelu, jonka avulla koneita ja käyttäjiä on helppo hallita isoissakin ympäristöissä. Palveluiden vikaantuminen voi kuitenkin aiheuttaa suurta taloudellista vahinkoa, jos käyttäjät eivät voi hyödyntää palvelun tarjoamia resursseja.

Tutkintotyön aiheen sain työnantajani tarpeesta, sillä Active Directoryn palvelut ovat tärkeä osa asiakkaidemme tietotekniikkaympäristöä. Tarkoituksena on ollut luoda kattava kuvaus siitä, mitä pitää tiedostaa, jotta voidaan olla todella varautuneita Active Directoryn katastrofitilanteeseen, ja miten siitä toivutaan mahdollisimman nopeasti. Työssä ei käsitellä Active Directoryn normaalia vianselvitystyötä, vaan keskitytään siihen, että kaikki ”tavallinen” on jo kokeiltu ja ainoa mahdollisuus on turvautua varmuuskopioihin.

Tutkintotyössä tutustutaan Active Directoryn rakenteeseen sekä sen tärkeimpiin komponentteihin. Työssä käydään läpi mitkä Active Directoryn osat pitää sisällyttää varmistuksen piiriin ja mitkä valinnat sekä ratkaisut vaikuttavat palvelinten vikasietoisuuteen. Lisäksi käydään läpi erilaisia varmistusohjelmia, nauhajärjestelmiä ja näiden ominaisuuksia. Työssä selvitetään myös eri palautuskäytännöt Active Directoryn osille. Työn lopussa on liitteenä toipumissuunnitelma, joka kuvaa Yritys X:ää, jonka Active Directory -ympäristössä ei ole käytössä yhtään toimivaa ohjauspalvelinta. Työn tarkoituksena on siis selvittää järjestelmäylläpitäjille, mitkä asiat vaikuttavat Active Directory -ympäristön toimivuuteen, ja miten se pitäisi varmistaa katastrofitilanteen varalta.

Avainsanat: Active Directory Nauhavarmistus Varmuuskopio Palautus

Sisällysluettelo

Johdanto

Active Directory -palvelu on Microsoftin keskitetty hallintaratkaisu yrityksille ja yhteisöille. Active Directory -palvelut ovat parhaimmillaan isoissa työasemaympäristöissä, missä pitää keskitetysti hallita niin käyttäjiä, tietokoneita kuin erilaisia resurssejakin.

Työ käsittelee toimintatapoja, miten Active Directoryn ohjauspalvelin saadaan palautettua katastrofitilanteen jälkeen toimintaan. Ohjelma- tai rautavian aiheuttama tietokantavika tekee ohjauspalvelimesta toimintakelvottoman ja estää sitä käynnistymästä normaalisti. Toinen katastrofitilanteen aiheuttaja on inhimillinen erehdys, missä järjestelmäylläpitäjän tekemä virhe replikoituu toisille yrityksen toimialueen ohjauspalvelimille.

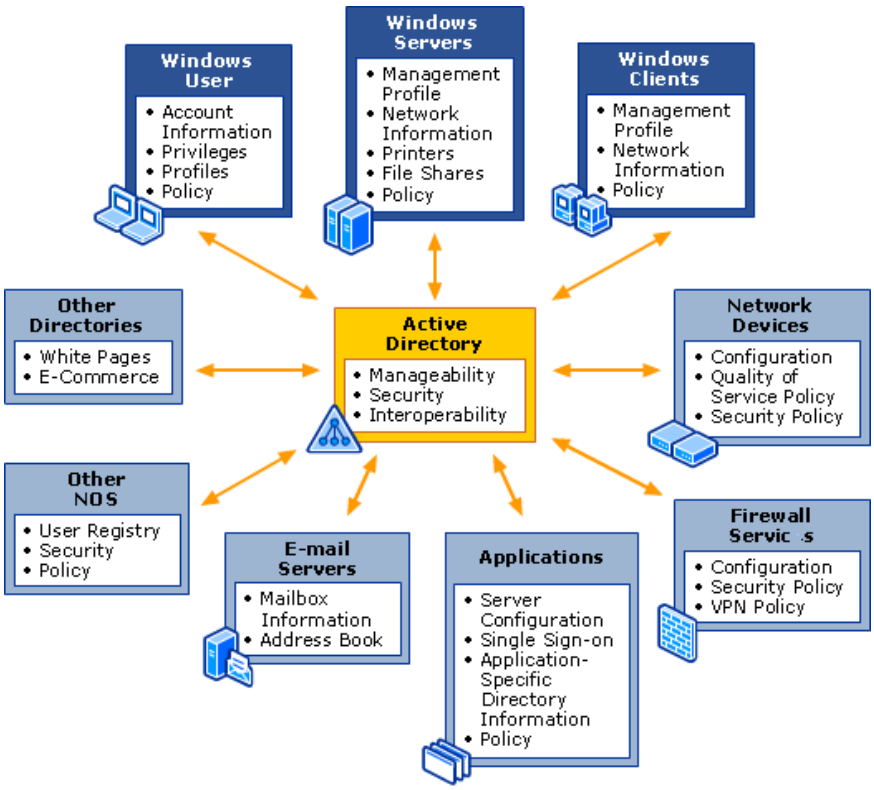
Työn aihe tuli asiakasyritykseltä, joka halusi selvittää Active Directoryn varmistamiseen liittyviä osatekijöitä ja tuoda järjestelmäylläpitäjien tietoisuuteen, mitä vahinkoa voi sattua ja kuinka paljon se aiheuttaa työtä, jos ollaan huolimattomia tai tietämättömiä, mitä ollaan tekemässä.

Työssä käydään ainoastaan läpi ohjauspalvelimella olevan Active Directory -palvelun katastrofitilanteen ennakointia ja siitä toipumista. Jos palvelimelle on asennettu jokin toinen palvelu, kuten DNS tai IIS, voidaan tarvita erilaisia toimenpiteitä, joita ei tässä työssä käsitellä. Silti tämän työn keskeinen sisältö pitää paikkansa, vaikka yrityksillä on käytössä erilaisia varmistusratkaisuja. Työssä oletetaan, että lukijalla on jonkin verran ennakkotietämystä Active Directorysta ja siihen liittyvistä asioista. Työssä ei myöskään käsitellä tavallista Active Directoryn ongelmanselvitystä, vaan oletetaan, että kaikki yleiset ratkaisumahdollisuudet on kokeiltu ja Active Directory ei silti toimi eikä näin ollen voi palvella ympäristöä. Järjestelmäylläpitäjät voivat hyödyntää työn lopussa liitteenä olevaa katastrofisuunnitelmaa tehdessään oman yrityksen Active Directory -ympäristöstä katastrofisuunnitelmaa.

1 Active Directory

1.1 Yleiskuvaus

Active Directory on Windows 2000/2003 Server - aktiivihakemistopalvelu, joka on käyttöjärjestelmän olennaisin osa. Active Directory –palvelu tarjoaa keskitettyjä hallintaratkaisuja niin käyttäjiin, sertifikaatteihin, työasemiin, tulostimiin sekä erilaisiin ryhmäkäytäntöihin, kuten kuvassa 1 tuodaan esille.



Kuva 1. Active Directoryn yleiskuvaus ([1@][CMS Consulting])

Termit ”hakemisto” ja ”hakemistopalvelut” viittaavat yleisiin tai yksityisiin verkossa oleviin hakemistoihin. Hakemisto on verkon objekteja sisältävä tietokanta. Hakemisto sisältää verkon resursseja koskevia tietoja, mikä tekee niiden löytämisen ja hallitsemisen helpommaksi.

Active Directoryyn sisältyy hakemisto, johon kaikki verkon resursseja koskevat tiedot tallennetaan. Active Directoryn tehtävänä on vähentää ylläpidettävien hakemistojen määrää, koska

käyttäjien, tietokoneiden ja sovellusten hallinta voidaan tehdä yhtenäisellä työkalulla. (Kivimäki 2004: 6.)

Active Directoryn pohjana toimii LDAP -protokolla. LDAP on johdettu OSI X.500 -hakemistomallista, mikä mahdollistaa tiedon helpon muokkaamisen ja hakemisen hajautetuista hakemistoista. LDAP -palvelut ja Active Directory ovat molemmat hierarkkisia hakemistoja, joihin voidaan tallentaa tietoja objekteista sekä niihin liittyvistä ominaisuuksista.

1.2 Active Directoryn rakenne

1.2.1 Nimiavaruus

Active Directoryn rakenteeseen liittyy useita tärkeitä tekijöitä. Yhtenä tärkeimmistä on DNS -nimiavaruuden suunnittelu, joka sisältää luottosuhteet ja toimialuehierarkian. Active Directoryn toiminnassaan käyttämä DNS -järjestelmä organisoi toimialueen tietokoneet järjestelmälliseksi kokonaisuudeksi. Itse DNS -toimialue ei kata tietokoneiden hallinnollista ryhmittelyä hakemistotietokannan perusteella, mutta tietokoneiden hallinnollinen ryhmittely on kuitenkin sidoksissa DNS -toimialueen nimihierarkiaan. (Kivimäki 2004: 13.)

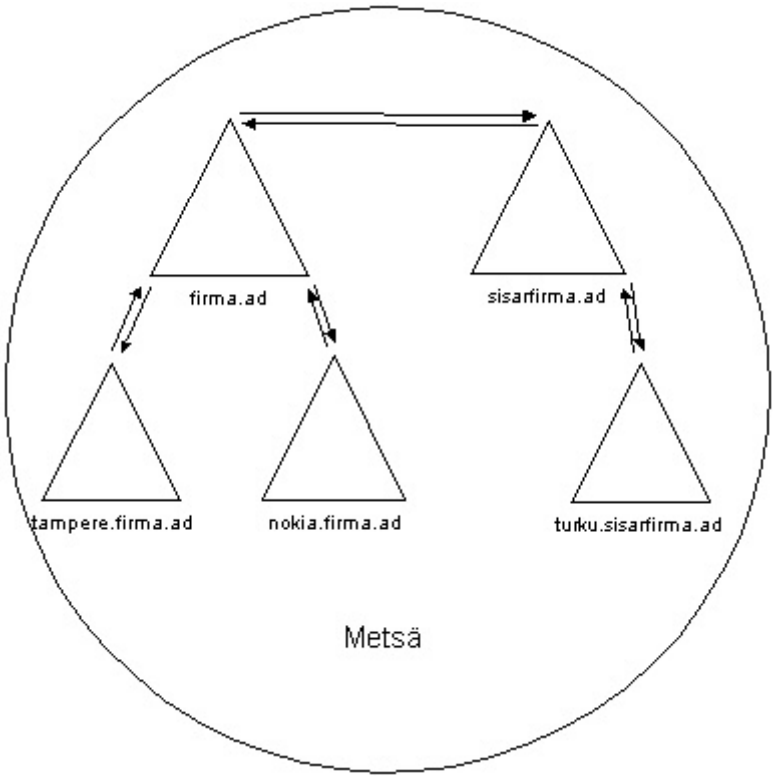
Nimiavaruus määrittää yrityksen juuritason toimialueen (Root Domain). Yksi tärkeimmistä päätöksistä nimiavaruutta luotaessa on se, onko Active Directoryn DNS -nimiavaruus sama kuin yritykselle tai yhteisölle rekisteröity Internet-toimialuenimi, esimerkiksi firma.com. Mikäli nimiavaruus on sama sekä julkisessa että sisäisessä verkossa, on huomioitava, että asiakaskoneiden on voitava luoda yhteys verkon sisäisiin ja ulkoisiin palvelimiin. Yleisin näistä ulkopuolisista palveluista on Internet-nimenselvitys. (Kivimäki 2004: 13.)

Yleensä sisäiset resurssit halutaan kuitenkin pitää turvallisuussyistä erillään julkisesta verkosta. Kyseinen toimintatapa mahdollistaa eriävän nimeämiskäytännön yksityisessä verkossa, esimerkiksi firma.ad. Näin yrityksen sisäiselle toimialueelle on mahdotonta päästä suoraan Internetistä käsin, sillä ulkopuolisilla nimipalvelimilla ei ole tietoa yrityksen ad -päätteisen juuritoimialueen osoitteista. (Kivimäki 2004: 14.)

Jokaisen tietokoneen sijainti verkossa voidaan päätellä sen täydellisestä DNS -nimestä, jota kutsutaan myös FQDN -nimeksi (Fully Qualified Domain Name) (Kivimäki 2004: 841). DNS -

palvelu kääntää toimialue- ja tietokonenimet IP -osoitteiksi, minkä ansiosta voidaan toimialueella viitata kyseiseen tietokoneeseen sen DNS -nimellä. DNS -nimi voi olla muotoa: ws123.firma.ad, jossa ws123 tarkoittaa yksittäisen koneen nimeä, firma organisatorista toimialuetta ja Active Directory -juuritoimialuetta.

Ensimmäinen toimialue, joka luodaan, on automaattisesti juuritoimialue. Tämän tapahtuman yhteydessä syntyy myös uusi ns. metsä, jonka ensimmäinen toimialuepuun juuri kyseinen toimialue on. Metsä saa saman nimen, kuin sen ensimmäinen toimialue. Juuritoimialue voi sisältää yhden tai useamaan lapsitoimialueen (child domain). Ennen kuin voidaan luoda lapsi- tai alitoimialueita, pitää juuritoimialueen olla luotuna. Toimialuepuun juuritoimialueeksi voidaan määritellä vaikka firma.ad ja kyseisellä toimialueella on lapsitoimialueina tampere.firma.ad ja nokia.firma.ad. Jos samaan metsään halutaan myöhemmin luoda uusi toimialue nimeltään sisarfirma.ad, syntyy metsään uusi toimialuepuu, jonka nimiavaruus ei ole yhtenevä firma.ad toimialueen kanssa. (Kivimäki 2004: 16)



Kuva 2. Metsän rakenne

Kaikki toimialueet kuuluvat kuitenkin samaan metsään (Kuva 2), jonka juuritoimialueena toimii firma.ad. Juuritoimialueen ja sen alitoimialueiden välisen luottosuhteen ansiosta resurssit ovat ko-

ko toimialuepuun käytettävissä. Juuritoimialueen ja muiden ylimmän tason toimialueiden välillä on luottosuhde, aivan samoin kuin ylemmän tason toimialueen ja alitoimialueen välillä on luottosuhde. Tämä mahdollistaa sen, että kaikki resurssit ovat periaatteessa koko toimialuepuuryhmän laajuisesti käytössä, vaikka toimialuepuuryhmä sisältääkin erinimisiä toimialueita. (Kivimäki 2004: 16.)

Toimialueen sisällä resursseja järjestellään organisaatioyksikköjen (OU, Organizational Unit) avulla. Organisaatioyksikköjen tulisi kuvastaa yrityksen organisaatiorakennetta. Organisaatioyksikköjä voidaan luoda, kun halutaan delegoida käyttäjäryhmiä, käyttäjiä ja resursseja koskevia järjestelmähallinnallisia oikeuksia. Organisaatioyksiköt tulee järjestellä loogiseksi rakenteeksi, joka sopii yrityksen toimintatapaan ja rakenteeseen. (Kivimäki 2004: 17.)

1.2.2 Toimipaikkarakenne

Ideaalisessa maailmassa tietoverkkojen välinen kommunikaatio tapahtuu nopeasti ja luotettavasti. Myös Active Directory-verkkoympäristön fyysiseen rakenteeseen on syytä kiinnittää huomiota. Toimipaikka (site) muodostuu yhdestä tai useammasta IP -aliverkosta. Toimipaikan rajat ovat usein samat kuin lähiverkon (LAN) tai nopean laajaverkon (WAN) rajat. (Kivimäki 2004: 17)

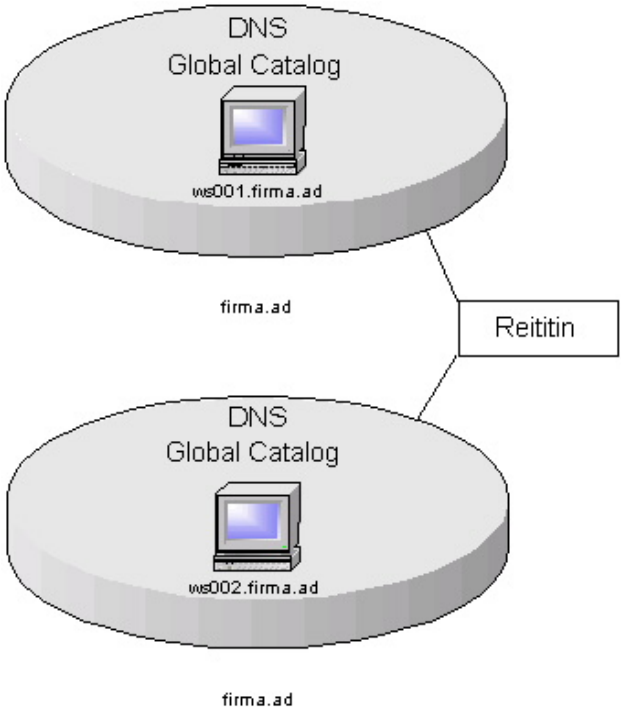
Toimipaikkarakennetta hyödynnetään yleensä, kun toimialueen tietokoneet on yhdistetty toisiinsa hitailla verkkoyhteyksillä. Yleensä tämä tarkoittaa organisaatioiden etätoimipisteitä tai tytäryhtiöitä. Verkon tietokoneet löytävät resurssit, kuten ohjauspalvelimet, tulostimet ja kotihakemistot, jotka sijaitsevat fyysisesti lähellä tietokonetta. Käyttäjän kirjautuminen toimialueelle ja objektien löytyminen nopeutuu ja vähentää verkkoliikennettä WAN -linkkien yli. (Kivimäki 2004: 931.)

Ohjauspalvelinten välillä tapahtuu replikointia, jos toimialue ja metsä ulottuvat useamman toimipisteen alueelle. Koska toimialueen ohjauspalvelimet replikoivat tietoja keskenään ja metsän sisällä tapahtuu yleisen luettelon (Global Catalog) replikointia, on oltava menetelmä, jolla replikointi voidaan järjestää tapahtuvaksi toimipaikkojen välillä. (Kivimäki 2004: 931.)

Oman ohjauspalvelimen sijoittaminen toimipaikkaan tarjoaa paikallisia palveluita. Kopio yleisestä luettelosta (Global Catalog)

nopeuttaa kirjautumista ja objektien löytymistä. Ohjauspalvelin voi toimia myös Active Directoryn DNS -palvelimena, jonka tietojen replikointiin käytetään hyväksi Active Directoryn replikointia. (Kivimäki 2004: 931.)

Kun metsän ensimmäinen ohjauspalvelin asennetaan, muodostuu samalla ensimmäinen toimipaikka nimeltä Default-First-Site-Name. Kyseiseen toimipaikkaan asennetaan kaikki ohjauspalvelimet, jos muita toimipaikkoja ei ole määritelty. Toimipaikkarakennetta ei siis tarvitse välttämättä määritellä. Verkot voidaan yhdistää toisiinsa silta (bridge) tyyppisen ratkaisun avulla, jolloin on mahdollista käyttää samaa aliverkkoaluetta verkon eri fyysisissä osissa. Suositeltavampaa on määrittää omat aliverkot verkon eri fyysisille osille. Kyseisessä määrittelyssä käytetään edelleen yhtä toimipaikkaa (Defaul-First-Site-Name –toimipaikka), mutta verkot yhdistetään toisiinsa reitittimien avulla. Tällaisessa ratkaisussa kummassakin aliverkossa voidaan käyttää samaa DNS –palvelinta, tai kummassakin aliverkossa voi olla oma DNS –palvelimensa. Active Directoryn automaattisesti muodostuvaa replikointitopologiaa ei voida käyttää, koska se perustuu juuri toimipaikkojen käyttämiseen. (Kivimäki 2004: 935.)



Kuva 3. Toimipaikkojen yhdistäminen toisiinsa.

Kuvan 3 tapauksessa on käytössä kaksi toimipaikkaa, jossa eri aliverkot on yhdistetty reitittimen avulla. Win2000/XP/2003 -asiakastietokoneet osaavat automaattisesti etsiä DNS -

palvelimesta oman toimipaikkansa resursseja ja ohjauspalvelimen. Global Catalog on käytössä molemmissa toimipaikoissa. Nyt voidaan hyödyntää Active Directoryn omaa replikointitopologiaa, tarvitsee toimipaikkarakennetta toimiakseen. (Kivimäki 2004: 933.)

Toimipaikkayhteyksien määrittelemiseen ja optimoimiseen käytetään hyväksi KCC -työkalua, joka luo vähiten kustannuksia tuottavan replikointitopologian. KCC luo toimipaikan sisällä jokaista hakemiston osiota varten rengastopologian, joka minimoi ohjauspalvelinten välisten siirräntävälien määrän. KCC luo puurakenteen kaikista toimipaikkojen välisistä yhteyksistä. KCC käynnistyy oletusarvoisesti 15 minuutin välein, mikä on tärkeä seikka myöhemmin käsiteltävää katastrofitilannetta ajatellen. (Kivimäki 2004: 936.)

Sillanpääpalvelinten (Bridgehead Server) tehtävänä on huolehtia Active Directoryn replikoinnista toimipaikkojen välillä. Oletusarvoisesti Intersite Topology Generator (ISTG) valitsee sillanpääpalvelimet automaattisesti jokaisessa toimipaikassa. ISTG toimii oletuksena jokaisen toimipaikan ensimmäisessä ohjauspalvelimessa. (Kivimäki 2004: 938.)

1.3 FSMO-roolit

Ohjauspalvelimet suorittavat Active Directory -toimialueissa monia erilaisia tehtäviä. Osalla ohjauspalvelimista on kuitenkin eriäviä tehtäviä, joita muut ohjauspalvelimet eivät saa suorittaa. Näitä ohjauspalvelimia kutsutaan Operations master -ohjauspalvelimiksi tai nimellä Flexible Sigle Master Operations (FSMO). Koska operations master -ohjauspalvelimet ovat kriittisiä hakemiston pitkän aikavälin toiminnan kannalta, niiden pitää olla kaikkien palveluita tarvitsevien ohjauspalvelinten ja asiakkaiden käytettävissä. Jotta eri operations master -rooleissa olevat ohjauspalvelimet voivat suorittaa niille määrättyjä tärkeitä tehtäviä, pitää niiden olla sijoitettuina paikkoihin, joissa verkko toimii luotettavasti ja on aina käytettävissä. (Kivimäki 2004: 723)

Roolit voidaan jakaa vielä kahtia, forest-wide operations master -rooliin ja domain-wide operations master -rooliin. Forest-Wide operations master -roolilla tarkoitetaan nimensä mukaisesti kaikkia niitä tehtäviä, jotka koskettavat koko Active Directory metsää. Domain-Wide operations master -roolilla tarkoitetaan tehtäviä, jotka koskettavat ainoastaan yhtä toimialuetta.

Kun ensimmäistä ohjauspalvelinta asennetaan uuteen metsään, muodostetaan kyseiset Active Directoryn osiot:

- Schema Directory Partition – Kaavaosio
- Domain Directory Partition – Toimialueen osio
- Ntds.dit – Mallitietokanta
- Schema Container – Kaavasäiliö
- Configuration Container – Konfiguraatiosäiliö
- Configuration Directory – Konfiguraatio-osio

(Kivimäki 2004: 723.)

1.3.1 PDC Emulator (Domain-Wide Operations Master)

PDC -emulaattorin (Primary Domain Controller) tehtävänä on emuloida pääohjauskonetta PDC:tä. PDC -emulaattorina toimiva kone käsittelee Windows NT 4.0 -varaohjauspalvelimilta tulevat replikointipyynnöt. Active Directoryn ollessa asennettuna seka-toimialuetilassa (Mixed Mode Domain), tarvitaan systeemi välittämään käyttäjätilien muutokset ja tiedot Windows NT -varaohjauspalvelimille. LAN Manager -replikointi hoitaa tämän asian. Jos toimialueessa on käytössä Windows 2000/2003 -oletustoimialue (Native Mode), ei kyseistä palvelua ole saatavilla. PDC -emulaattori asentuu toimialueen ensimmäiselle ohjauskoneelle, johon se myös jätetään. PDC -emulaattoria ei suositella toimivaksi samassa palvelimessa Infrastructure master -palvelun kanssa. Infrastructure Master -palveluun palataan kohdassa 1.3.5. (Kivimäki 2004: 732.)

Käyttäjän vaihtaessa salasanaa millä tahansa ohjauspalvelimella lähetetään pyyntö PDC -emulaattorille. Kyseinen käytäntö on hyödyllinen, jos käyttäjä välittömästi salasanan vaihdon jälkeen yrittää kirjautumista verkkoon eikä uusi salasana ole vielä replikoitunut kaikille ohjauspalvelimille. Tällöin kirjautumista vastaanottava palvelin tarkistaa PDC -emulaattorilta, onko käyttäjällä käytössä uudempi salasana. Vaihdettu salasana replikoituu normaalisti muihin ohjauskoneisiin. Emulaattori käsittelee myös käyttäjätilien ja tietokonetilien lukitsemisen. Jos kirjautumisessa on ongelma, ohjauspalvelin tarkistaa PDC -emulaattorilta, onko syynä tilin lukkiutuminen. (Kivimäki 2004: 732.)

PDC -emulaattori on pakollinen synkronoitaessa aikaa koko metsän tasolla. Windows 2000 sisältää W32time – aika -palvelun, jota käyttää hyväksi myös Kerberos autentikointiprotokolla. Kaikki Windows 2000 koneet metsässä käyttävät yhteistä aikaa. Tämän palvelun tarkoitus on taata, että aikapalvelu käyttää hierarkkista suhdetta, joka kontrolloi auktorisointia ja takaa

yhteisen ajan. Metsän juuritoimialueen PDC -emulaattori pitää synkronoida ulkoista vakioaikalähdettä vasten, sillä se välittää päivitykset muille toimialueen ohjauspalvelimille. ([2@][Microsoft])

1.3.2 RID Master (Domain-Wide Operations Master)

RID (Relative Identifier) Master -palvelin varaa suhteellisia suojaustunnisteita kaikille toimialueen ohjauspalvelimille. Aina kun toimialueen palvelin luo Security Principalin, esim. käyttäjä, ryhmä tai tietokoneobjektin, se liittää objektiin yksilöidyn Security Identifierin (SID). SID koostuu toimialueen SID:istä, joka on sama kaikilla toimialueella luotavilla security principaleilla ja RID:stä, joka on yksilöllinen jokaisella security principalilla, joka luodaan toimialueelle. (Kivimäki 2004: 734.)

Jokaisella ohjauspalvelimella on RID -tunnisteiden varanto. Vapaana olevien RID -tunnisteiden määrän laskiessa alle 100, pyytää kyseinen ohjauspalvelin toimialuekohtaiselta RID Master -palvelimelta 500 uutta vapaata RID -tunnistetta. Tämän käytännön ansiosta jokaisella ohjauspalvelimella pitäisi aina olla 100 – 600 vapaata RID -tunnistetta. (Kivimäki 2004: 734.)

RID Masteria käytetään myös silloin, kun objekteja siirretään toimialueesta toiseen. Siirto pitää tehdä lähtötoimialueen RID Master -palvelimella. Tämän vaatimuksen ansiosta Active Directory takaa sen, ettei kaksi ylläpitäjää voi siirtää samaa objektia kahteen eri toimialueeseen yhtä aikaa. Kyseinen ristiriita johtaisi siihen, että kaksi identtistä objektia käyttäisi samaa GUID:ia (Global Unique Identifier). (Kivimäki 2004: 735.)

1.3.3 Domain Naming Master (Forest-wide Operations Master)

Domain Naming Masteria käytetään toimialueiden poistamiseen ja lisäämiseen. Kyseinen rooli on metsäkohtainen ja sijaitsee oletuksena ensimmäisessä asennetussa ohjainpalvelimessa. Palvelimen vastuulla on muun muassa huolehtia siitä, että jokainen toimialuenimi on yksilöllinen. Myös viittaukset ulkoisiin hakemistoihin kulkevat Domain Naming Masterin kautta. (Kivimäki 2004: 740)

1.3.4 Schema Master (Forest-Wide Operations Master)

Active Directoryn sydämessä on kaava (schema), jota voidaan pitää kaikkien objektien ja säiliöiden pohjakuvana. Kaavan pitää olla sama koko metsän laajuisesti, mistä johtuen vain yksi Schema Master -ohjauspalvelin voi hyväksyä kaavaan tehdyt muutokset. Oletuksena Schema Master asentuu metsän ensimmäiselle ohjauspalvelimelle. Schema Master -palvelimen pitää olla verkossa käytettävissä, kun muutoksia kaavaan tehdään. Muutoksia tekevällä ylläpitäjällä pitää olla myös oikeus kirjautua tähän kyseiseen palvelimeen. Kaavaan tehdyt muutokset replikoidaan jokaiseen metsän ohjauspalvelimeen. (Kivimäki 2004: 737.)

1.3.5 Infrastructure master (Domain-Wide Operations Master)

Infrastructure masteria käytetään päivittämään objektiviittauksia (object reference) toimialueessa, joka osoittaa objektia toisessa toimialueessa. Objektiviittaus sisältää objektin globally unique identifierin (QUID), distinguished namen (DN) ja mahdollisesti myös SID:n. Kun objekti viittaa toiseen objektiin, jota ei löydy toimialueen ohjauspalvelimen hakemistotietokannasta, esimerkiksi, kun se sijaitsee toisessa toimialueessa, käytetään erikoista tietuetta, jota kutsutaan varjotietueeksi (phantom).
(Kivimäki 2004: 736.)

Varjotietuetta tarvitaan hakemistotietokannassa edustamaan kyseistä viitattua tietuetta. GUID ei koskaan muutu. DN muuttuu, jos objektia siirretään tai uudelleen nimetään. SID muuttuu ainoastaan siinä tapauksessa, että se siirretään toimialueesta toiseen. Tästä johtuen SID ja DN tunnisteet pitää päivittää varjotietueessa. (Kivimäki 2004: 736.)

Toimialueen Infrastructure master -palvelun vastuulla on päivittää varjotietue siirron tai uudelleen nimeämisen jälkeen. Palvelun tarvitsee myös replikoida muuttuneet varjotietueet muille saman toimialueen ohjauskoneille. Infrastructure master -palvelu suorittaa hakemistotietokannasta jaksollisia tarkistuksia viittauksista, jotka eivät ole sen omassa tietokannassa, koska ne sijaitsevat joko toisessa toimialueessa tai metsässä. (Kivimäki 2004: 736.)

Palvelu ottaa myös yhteyttä Global Catalog -palvelimeen tarkistaakseen, että tämän viittaukset pitävät paikkansa. Infrastructure master asentuu oletuksena metsän ensimmäiseen ohjauskoneeseen. Suosituksena on, ettei Global Catalog -palvelu sijaitse samassa koneessa kuin Infrastructure master -palvelu.
(Kivimäki 2004: 736.)

1.4 Global Catalog

Yleinen luettelo eli Global Catalog (GC) on palvelu, jossa säilytetään tieto kaikista objekteista metsän laajuisesti. Global Catalog on tärkeässä roolissa, kun halutaan selvittää jonkin objektin olemassaolo metsänlaajuisesti. Käyttäjä voi siis etsiä erilaisia objekteja Active Directorystä, kuten käyttäjiä, palvelimia ja tulostimia. Hakutoiminto auttaa myös siksi, että LDAP -nimet ovat monimutkaisia ja vaikeasti muistettavia, kun taas Global Catalogista voidaan hakea erilaisten hakukriteerien avulla.
(Kivimäki 2004: 692.)

Global Catalog sisältää tiedot kaikista metsän objekteista, mutta vain osan niiden attribuuteista. Active Directoryn kaava (Schema) sisältää yli 800 attribuuttia, mutta vain noin 140 niistä tallennetaan Global Catalogiin. Oletusarvona on, että yleiseen luetteloon tallennetaan vain kaikkein yleisimmissä hakutoiminnoissa käytetyt attribuutit (kuten etu- ja sukunimi, käyttäjätunnus) sekä attribuutit, joiden avulla löydetään obkjektin täydellinen replika. Lisäksi Global Catalogin avulla voidaan etsiä objektit tarvitsematta replikoida toimialueen kaikkia tietoja jokaiseen ohjauspalvelimeen. (Kivimäki 2004: 692)

Jokainen ohjauspalvelin ylläpitää luku/kirjoitusversiota kaikista niistä objekteista, jotka kuuluvat sen toimialueelle. Global Catalog -palvelua ylläpitävä ohjauspalvelin ylläpitää myös osittaista lukuversiota omasta, mutta myös koko metsän muiden toimialueiden objekteista. (Kivimäki 2004: 693.)

Global Catalogin luominen tapahtuu automaattisesti Active Directoryn replikointijärjestelmän muodostamana. Global Catalog aiheuttaa palvelimelle ylimääräistä kuormaa. On tärkeätä ottaa huomioon verkon rakenne ja kapasiteetti sekä käsitellä replikointi- ja kyselyliikennettä. Mitä useampi Global Catalog palvelin on käytössä, sitä varmempi ja nopeampi palvelu on käyttäjälle. Monen palvelimen käyttö lisää verkossa tapahtuvaa replikointiliikennettä. Objektien etsimisen lisäksi Global Catalogia käytetään kahdella tavalla käyttäjien kirjautumisessa ja autentikoinnissa toimialueella:

- Käyttäjä -objektin löytäminen UPN:n avulla

Ryhmäjäsenyyden tarkastaminen Universal-ryhmästä. (Kivimäki 2004: 693.)

Käyttäjän ensisijainen nimi (UPN, User Principal Name) on nimi, jota käytetään kirjautumisessa toimialueeseen. Nimi itsessään koostuu kahdesta osasta:

- Kirjautumistunnus (User logon name), esimerkiksi kai.stenvik
- Käyttäjän ensisijainen nimen jälkiliite (UPN suffix), DNS -toimialuenimi tai -jälkiliite, esimerkiksi firma.ad

Käyttäjätiliä (objektia) siirrettäessä metsän sisällä kirjautumistunnus säilyy samana. Tästä on se etu, että riippumatta toimialueesta, missä käyttäjä on määritelty, käyttäjän kirjautumistunnus säilyy samana. (Kivimäki 2004: 441.)

Universal -ryhmiä käytetään määriteltäessä monien toimialueiden toisiinsa liittyvien resurssien käyttölupia. Universal -ryhmille voidaan antaa käyttöoikeuksia resursseihin, jotka sijaitsevat muulla toimialueella, kuin mihin ryhmä on luotu. Käyttäjän kirjautuessa toimialueelle tarkistetaan tämän Universaali-ryhmäjäsenyytensä Global Catalog -palvelulta. Mikäli Global Catalog -palvelu ei ole käytettävissä, käyttäjät eivät voi kirjautua toimialueelle ensimmäistä kertaa, elleivät ole Domain Admins -ryhmän jäseniä. Tämä johtuu siitä, että kirjautumisen yhteydessä tehtävän tarkistuksen takia käyttäjä ei voi saada pääsyä resursseihin, joihin universaalilta ryhmältä on pääsy evätty.
(Kivimäki 2004: 693.)

Universaalit ryhmät voidaan ottaa kuitenkin käyttöön paikallisesti määrittelemällä asetus ”Enable Universal Membership Caching”. Vaikka universaalit ryhmät eivät olisi paikallisessa käytössä, voivat käyttäjät kirjautua toimialueelle, jos he ovat kirjautuneet jo kerran aikaisemmin. Universal -ryhmiä suositellaan käytettäväksi vain silloin, kun jäsenyys on suhteellisen pysyvä. Muutoksia tehtäessä muutokset pitää replikoida kaikkiin Global Catalogeihin metsässä. (Kivimäki 2004: 693.)

1.5 Roolien sijoittaminen palvelimiin

Yleisenä toimintatapana tulisi pitää menettelyä, jossa vähintään yksi Global Catalog -palvelin sijoitetaan kuhunkin toimipaikkaan. Asiakaskoneet etsivät oletuksena resursseja oman toimipaikkansa alueelta, jolloin saadaan se etu, ettei toimipaikkojen välinen verkkoyhteys rasitu liikaa. Mikäli verkkoyhteys on todella ruuhkainen eikä jokaisella toimipaikalla ole määritettynä Global Catalogia, saattaa asiakkailla ilmetä kirjautumisongelmia. Mikäli toimipaikassa on useampi ohjauspalvelin, olisi ihanteellista määrittää vähintään kaksi palvelinta kussakin toimipaikassa pitämään

Global Catalogia. Näin järjestelmään saataisiin vikasietoisuutta ja kuormantasausta. Mikäli olemassa on vain yksi toimialue, ei myöskään kaikkien ohjauspalvelinten määrittäminen Global Catalog -palvelimiksi aiheuta vielä ylimääräistä kuormaa verkolle, koska replikointitopologian muodostaminen ja replikointiliikenne pysyvät yhden toimialueen ja -paikan sisällä. (Kivimäki 2004: 693 – 694.)

Global Catalog -palvelimet pitäisi sijoittaa verkkoon niin, että ne ovat nopean ja luotettavan yhteyden päässä toimialueiden Infrastructure Master -palvelimiin. Tämä siksi, että kyseisen roolin omaava palvelin tarvitsee Global Catalog -tietoja objektiviittausten päivittämiseen. Infrastructure Master -palvelun sijoittamista samaan palvelimeen Global Catalog -palvelun kanssa pitäisi välttää, mikäli toimialueella on enemmän kuin yksi ohjauspalvelin. Muutoin Infrastructure Master ei löydä vanhentuneita hakemistotietoja, sillä se vertaa tietojaan itseään vasten. (Kivimäki 2004: 743.)

Metsäkohtaiset roolit, kuten Domain Naming Master ja Schema Master, kannattaa jättää oletuksena olevalle metsän ensimmäiselle ohjauspalvelimelle, sillä niiden siirtäminen toisille palvelimille aiheuttaa lisätyötä eikä varsinaista suorituskykyä saada parannettua. Oletuksena Domain Naming Master toimii samassa palvelimessa kuin Global Catalog, ja nämä roolit onkin syytä jättää saman palvelimen hoidettavaksi. Tämä johtuu siitä, että toimialueiden nimeämistilanteissa täytyy Domain Naming Masterilla olla esteetön pääsy Global Catalogiin objektien nimien yksilöllisyyden varmistamiseksi. (Kivimäki 2004: 746.)

Toimialuekohtaiset roolit, PDC-, Infrastructure- ja RID Master-roolit tulisi jättää alkuperäiselle palvelimille muilla toimialueilla paitsi metsän juuritoimialueella. Näiden palveluiden sijaitseminen samalla palvelimella ei yleensä aiheuta merkittävää lisäkuormaa metsän juuritoimialuetta lukuun ottamatta. Metsän juuritoimialueella toimialuekohtaiset roolit tulisi siirtää pois oletuspalvelimelta, jotta toiminnan sujuvuus saadaan varmistettua ja ohjauspalvelinten rasitus hajautettua. (Kivimäki 2004: 746.)

RID Master ja PDC toimivat yhdessä parhaiten samalle palvelimelle määritettynä, koska PDC tarvitsee suhteellisia tunnisteita muita ohjauspalvelimia enemmän. PDC-emulaattori -rooli vaatii ohjauspalvelimelta eniten suorituskykyä, koska se on suurimmassa päivittäisessä käytössä, johtuen sen suurimmasta yksittäisten toimintopalvelinten tehtävämäärästä. Tästä johtuen kyseisen palvelimen tulisi olla riittävän tehokas suhteutettuna verkon käyttöasteeseen. (Kivimäki 2004: 747 – 748.)

1.6 Group Policy

Group Policy eli ryhmäkäytäntö on järjestelmän kokoonpanoasetus, jonka avulla voidaan hallita verkkoon liittyviä määrityksiä keskitetysti. Group Policy -määrityksillä hallitaan käyttäjiä että tietokoneita. Ryhmäkäytännöt voidaan kohdistaa yksittäiseen tai useisiin toimialueisiin, toimialueiden alaryhmiin tai paikallisiin järjestelmiin. Group Policy -määrityksen avulla voidaan hallita ja asettaa erilaisia ominaisuuksia (Kivimäki 2004: 595 - 599):

- Security Settings: suojauskäytännöt ohjaavat tietokoneen tietoturvan kannalta keskeisiä asetuksia. Määrityksien avulla voidaan määrätä salasana, työaseman lukitus ja Kerberos -käytäntöjä. Security Settings:in avulla voidaan myös rajoittaa, ketkä kuuluvat rajoitettuihin ryhmiin, ja mitkä Windows -palvelut (verkko, tiedosto, tulostus, Internet…) käynnistyvät koneen käynnistyksen yhteydessä.

- Administrative Templates: rekisteriperusteiset ryhmäkäytännöt, mallitiedostot, joiden avulla määritetään käyttöjärjestelmäkomponentit sekä työpöydän käyttäytymistä ja ulkoasua ohjaavat asetukset.

- Scripts: järjestelmävalvojat voivat määrittää erilaisia skriptejä ja komentotiedostoja, jotka ajetaan järjestelmän käynnistyessä (Startup) tai sulkeutuessa (Shutdow), tai kun käyttäjä kirjautuu (logon) järjestelmään tai siitä ulos (logout).

- Software Settings / Software Installation: kyseiset määritykset vaikuttavat sovelluksiin, joihin käyttäjällä on käyttölupa. Käytäntöjä hyväksi käyttäen voidaan sovellusten asennus toteuttaa kahdella tavalla. Group Policy -määritys asentaa ja päivittää toimialueeseen kuuluvan työaseman sovellukset automaattisesti tai antaa mahdollisuuden tarjota käyttäjän käytettäväksi sovellus, jota hän ei voi poistaa. Toinen tapa on julkaista (Publish) sovellus Actice Directoryssa. Käyttäjälle annetaan tällä tavalla mahdollisuus itse asentaa tai poistaa sovellus ohjauspaneelin avulla. Sovelluksesta ei tule julkaistaessa
pikakuvakkeita käyttäjän työpöydällä (desktop), eikä paikallisia rekisterimuutoksia tehdä.

- Remote Installation Services (RIS): etäasennuspalvelua voivat käyttää työasemat, joiden verkkokortissa on mahdollisuus Pre-boot Execution Environment (PXE) etäkäynnistystoimintoon. Etäkäynnistystoiminnon avulla kone ottaa yhteyden verkossa olevaan RIS -palvelimeen asentaakseen käyttöjärjestelmän, RIS –palvelu tarkistaa tässä vaiheessa, mitkä Group Policy –määritykset vaikuttavat asennukseen.

- Internet Explorer Maintenence: tämän määrittelyn avulla vaikutetaan Internet Explorer -selaimen asetuksiin. Tämän avulla ylläpitäjä voi vaikuttaa selaimen ulkonäköön, määrittää ja hallita lähiverkon (local area network, LAN) yhteysasetuksia, asettaa oletuskotisivun käyttäjille, määrittää selaimen turvallisuustasot sekä vaikuttaa siihen, mitä Internet –pohjaisia sovelluksia käytetään esim. sähköpostin ja uutisryhmien lukemiseen.

- Folder Redirection: käyttäjien kansioiden uudelleenohjausta käytetään, kun halutaan ohjata joku erityisistä kansioista toiseen paikkaan. Nämä käyttäjäprofiilin alla tehtävät ohjaukset koskevat seuraavia kansioita:

  Ohjelmien tiedot (Application data)
  Työpöytä (Desktop)
  Omat tiedostot (My Documents)
  Käynnistä -valikko (Start Menu)

  Kansion uudelleenohjauksen avulla käyttäjille voidaan luoda mukana kulkevia profiileita (Roaming Profile), jolloin käyttäjä voi tallentaa tiedostot ”tietämättään” verkkoon levypalvelimelle. Näin tiedostot ovat käytettävissä mistä tahansa toimialueen tietokoneelta, eivätkä ole paikallisesti koneen kiintolevyllä. Kyseinen palvelu säästää suuresti hallinnointia sekä mahdollistaa keskitetyn varmistusjärjestelmän käytön.

  Group Policyn avulla tehdyt määritykset tallennetaan ryhmäkäytäntöobjektiin (Group Policy Object, GPO). GPO sisältää toimipaikkoja, toimialueita ja organisaatioyksikköjä koskevia asetuksia. GPO:n asetukset tallennetaan kahteen paikkaan:

  - Ryhmäkäytäntöjen säiliö (Group Policy Container, GPC) on Active Directoryn objekti. Tietokoneet voivat käyttää sitä löytääkseen Group Policyn mallit. GPC sisältää versiotietoa, jota hyväksi käyttäen ohjauspalvelimet vertaavat oman versionsa uutuutta. Jos versio ei

ole uusin saatavilla oleva, päivitetään se siltä ohjauspalvelimelta, jolla on uusin versio.

- Ryhmäkäytäntöjen mallit (Group Policy Template, GPT) on SYSVOL-kansiorakenne. Group Policy – objektia luotaessa järjestelmä luo vastaavan kansiorakenteen. Kansiorakenne sisältää tietoa Group Policyn avulla hallituista sovelluksista, suojauskäytännöistä ja scripteistä. (Kouti & Seitsonen 2002: 524.)

Group Policy -määritykset toimivat vain Windows 2000/XP/2003 -järjestelmissä. Määritykset käsitellään järjestelmän käynnistyessä. Toimipaikat, toimialueet ja organisaatioyksiköt eivät ole sidottuja yhteen GPO -objektiin, vaan objekteja voidaan linkittää Active Directoryn eri osiin. Kyseisen ratkaisun avulla Policyyn tehdyt myöhemmät muutokset tulevat voimaan kaikissa niissä Active Directoryn osissa, joihin objekti on linkitetty.

2 Active Directoryn varmistus ja vikasietoisuus

2.1 Yrityksen tarpeet

Järjestelmän vikatilanne ja alhaalla oloaika (down time) voi olla erittäin kallista nykyajan yrityksille. Yrityksen tietohallinto-osaston on varauduttava tiedettyihin ongelmiin, mutta sillä on oltava myös valmiudet toipua ja hallita ennakoimattomia ja erikokoisia järjestelmäkatastrofeja. Rahallinen menetys riippuu yrityksen toimialasta ja siitä, kuinka kriittinen kyseinen järjestelmä on tuottavuuden kannalta. Esimerkkinä voidaan käyttää paperikoneen pysähtymistä paperitehtaassa. Kyseinen vika voi maksaa miljoonia euroja tunnissa.

Tietojärjestelmiä hankittaessa yhtenä tärkeimpänä kriteerinä tietohallinnon näkökulmasta on tietenkin raha. Järjestelmäylläpitäjät haluaisivat ostaa aina parhaat ja kalleimmat laitteet sekä ohjelmistot. Missä raja kulkee? Aina kallein ja järein varmistusjärjestelmä ei ole paras, jos se on ylimitoitettu yrityksen tarpeisiin nähden. Tietenkin huippujärjestelmällä saadaan varmistettua tietojärjestelmät, mutta systeemin hankintahinta on todennäköisesti kallis ja vaatii henkilökunnan jatkuvaa koulutusta. Jos varmistusjärjestelmän käyttöaste on vähäinen sen kapasiteettiin nähden, hankinta on ollut mahdollisesti väärä. Haluttu käytettävyys ja riittävä varmistus olisi voitu toteuttaa helpommin ja halvemmilla kustannuksilla.

Jos halutaan kuitenkin varmistua, että yrityksen tuottavuuden kannalta tärkeät järjestelmät ovat jatkuvasti käyttäjien saatavilla ja ongelmatilanteista toipuminen on lähes läpinäkyvää käyttäjälle, pitää varmistusjärjestelmiin ja vikasietoisuuteen satsata. Säästö järjestelmän hankintavaiheessa voi olla tuhansia tai kymmeniä tuhansia euroja, mutta saatu rahallinen etu voi olla mitätön, jos järjestelmä on vikatilassa useita tunteja tai jopa päiviä. Toisin sanoen säästö väärässä paikassa voi maksaa myöhemmin todella paljon.

2.2 Active Directoryn varmistettavat osiot

Tärkeä osa Active Directoryn katastrofitilanteen toipumissuunnitelmassa on ymmärtää, mitä asioita pitää ottaa huomioon, kun AD ympäristöä varmistetaan.

Active Directory varmistetaan osana järjestelmän tilaa (System State). Järjestelmän tilalla tarkoitetaan toinen toisistaan riippuvaisia järjestelmäkomponentteja. Järjestelmäkomponentit pitää varmistaa ja palauttaa yhdessä. (Kivimäki 2004: 1001.)

Järjestelmäkomponentit, jotka muodostavat System State -tilan ohjauspalvelimessa ovat: (Kivimäki 2004: 1001: 1002):

- Järjestelmän käynnistystiedostot (System Start-up Files). Windows -palvelin tarvitsee näitä tiedostoja, jotta se voi käynnistyä. Nämä tiedostot varmistetaan automaattisesti järjestelmätietojen yhteydessä.

- Järjestelmärekisteri (System registry). Kopio järjestelmärekisteristä tallennetaan kansioon nimeltä %SystemRoot%\Repair\Regback, josta on mahdollisuus palauttaa pelkästään rekisteriarvot, jolloin ei tarvitse tehdä kokonaista System State –palautusta.

- Komponenttipalveluiden luokkarekisteritietokanta (Class registration database of COM+). Component Object Model (COM) on binäärimuotoinen standardi hajautetussa järjestelmäympäristössä toimivien komponenttiohjelmistojen kirjoittamista varten.

- SYSVOL järjestelmäasema toimii Active Directoryssä määritettynä oletusarvoisena tallennuspaikkana tiedostoille, joiden pitää olla jaettuna koko toimialueen käyttöön. Ohjauspalvelimen SYSVOL -kansiossa on seuraavat kohteet:

- Jaetut NETLOGON -kansiot. Kyseiset kansiot sisältävät yleensä käyttäjän kirjautumiskomentosarjat (logon scripts) ja ryhmäkäytäntöobjektit (GPO) asiakaskoneille, joissa on käytössä jokin muu käyttöjärjestelmä kuin Windows 2000.

- Tiedostojärjestelmän liittymäkohdat (File system junctions)

- Käyttäjän kirjautumiskomentosarjat Windows XP/2000 -asiakaskoneille sekä Windows 95-, Windows 98- ja Wndows NT 4.0 -asiakaskoneille.

- Windows XP/2000 ryhmäkäytäntöobjektit (GPO).

- Tiedostojen replikointipalvelu (File Replication Service, FRS). Palveluun on sijoitettu ne tiedostot ja hakemistot, joiden pitää olla käytettävissä ja synkronoituna ohjauspalvelinten välillä.

Active Directory. Active Directory sisältää seuraavat tiedostot:

- Ntds.dit: Active Directoryn tietokanta

- Edb.chk: Tarkistuskohdan tiedosto (checkpoint file).

- Edb*.log: Tapahtumalokit, kukin kooltaan 10 megatavua.

- Res1.log ja Res2.log: Varatut tapahtumalokit.

Ohjauspalvelimelle voi olla asennettuna Windows Clustering tai Certificate Services ja myös ne varmistetaan System State -tilan yhteydessä. (Active Directory Disaster Recovery White Paper 2000: 8.)

Jos käytetään Active Directoryyn integroitua DNS:ää, vyöhykkeen tiedot varmistetaan osana AD:n tietokantaa. Jos ei käytetä Active Directoryyn integroitua DNS:ää, vyöhykkeen tiedostot pitää varmistaa erikseen. Jos kuitenkin varmistetaan järjestelmälevyn (Systen disk) yhdessä System State -tilan kanssa, alueen tiedot varmistetaan osana järjestelmälevyä. (Kivimäki 2004: 1002.)

2.3 Active Directoryn hyvän varmistamisen osatekijät

Jotta Active Directoryn varmistuksesta olisi jotain hyötyä, tulee järjestelmäylläpitäjän käsittää, mitä asioita pitää ottaa huomioon tehtäessä varmistus. Ensimmäinen tärkeä seikka on sisältö. Hyvä varmistus sisältää ainakin System State -tilan, järjestelmälevyn sisällön ja SYSVOL -kansion, jos se ei ole järjestelmälevyllä. System State sisältää monia tärkeitä tietoja, joilla saadaan palautettua ohjauspalvelin. Järjestelmälevyn ja SYSVOL -hakemistorakenteen varmistus takaa, että kaikki tarvittavat järjestelmätiedot ja kansiot ovat paikoillaan käynnistettäessä palautusta. Parhaan suorituskyvyn takaamiseksi Microsoft neuvoo, että Active Directoryn lokien ja tietokantojen pitäisi sijaita eri levyillä. Ohjauspalvelimen ollessa asennettuna kyseisellä tavalla tietokannat ja lokit varmistetaan normaalisti System State -tilan mukana. (Active Directory Disaster Recovery White Paper 2000: 9.)

Jos varmistus on vanhempi kuin Active Directoryyn asennettu tombstone lifetime -aika, aiheuttaa tämä tiedostojen epäyhteneväisyysongelman. Tombstone -objekti ei ole replikoitunut palautetuille ohjauspalvelimille ennen sen vanhenemista ja näin objekti jää ainoastaan palautetulle ohjauspalvelimelle. Oletuksena tombstone lifetime -aika on 60 päivää. Joissakin ympäristöissä asetusta on pienennetty, jotta Active Directoryn tietokannan kokoa voidaan pienentää. Active Directory sisällyttää tombstone lifetime -ajan varmistus- ja palautusprosessiin ja näin suojaa itseään kyseistä tietojen epäyhtenäisyysongelmaa vastaan. Objektin poistaminen Active Directorystä tapahtuu kahdessa osassa. Kun objekti poistetaan Active Directorystä, objekti muuttuu tombstone -objektiksi, jota tämän jälkeen replikoidaan ympäristön muihin ohjauspalvelimiin, jotta nekin saavat tietää poistosta. Active Directory poistaa tombstone -objektin, kun tombstone lifetime on kulunut loppuun. (Kivimäki 2004: 1003.)

Tämän ansioista ohjauspalvelin pitää palauttaa ennen tombstone -objektin vanhenemista. Näin ollen varmuuskopion käyttökelpoinen ikä on sama kuin tombstone lifetime -aika. (Active Directory Disaster Recovery White Paper 2000: 10.)

Varmistuksien aikavälin pitäisi näin ollen olla tombsone lifetimen sisällä. Microsoft suosittelee, että System State -tila sekä järjestelmälevyt varmistettaisiin useammin. Näin voidaan taata, että

millä hetkellä hyvänsä on olemassa varmuuskopio, joka sisältää viimeisimmän tiedon. (Active Directory Disaster Recovery White Paper 2000: 10.)

On tärkeää tietää, että varmistettua dataa jostain ohjauspalvelimesta voidaan ainoastaan käyttää juuri sen palvelimen palauttamiseen. Toisen ohjauspalvelimen tiedoilla ei voida palauttaa toista ohjauspalvelinta. Kun halutaan varmistua, että koko ympäristö on varmistettu, pitää järjestelmäylläpitäjien varmistaa jokainen ohjauspalvelin. Tämä pitää ottaa huomioon, kun yrityksessä tehdään varmistus-suunnitelmaa. Vähintään pitäisi varmistaa kaikki Operations Master -roolin omaavat sekä Global Catalog -koneet. Myös juuritoimialueen ensimmäinen ohjauspalvelin pitäisi aina varmistaa. (Active Directory Disaster Recovery White Paper 2000: 10.)

2.4 Varmistusikkuna

Käytössä olevan ohjauspalvelimen varmistamiseen menevän ajan tuntemus on tärkeää suunniteltaessa varmistus strategiaa. Koska varmistus tehdään ohjauspalvelimen ollessa käytössä, varmistuksen aloitusaika ei ole niin tärkeä. Kuitenkin suositellaan, ettei varmistusta suoriteta työpäivän aikana, sillä se voi vaikuttaa Active Directoryn muiden ominaisuuksien käytettävyyteen. Yleisesti varmistukset ajoitetaan kaikista hiljaisimpaan hetkeen, mikä monessa yrityksessä tarkoittaa yöaikaa. (Active Directory Disaster Recovery White Paper 2000: 11.)

3 Active Directoryn varmistus- ja palautustyökaluja

Active Directory ja muu tietoverkkoympäristö asettaa haasteen valittaessa toimivaa varmistus- ja palautusratkaisua. Yleensä suuriin ja monimutkaisiin ympäristöihin valitaan keskitetty ratkaisu, jonka etuja ja haittoja ovat:

+ tietoturva
+ varmistusohjelmiston hallinta
+ varmistuksien/palautusten keskitetty hallinta
+ yksi varmistusohjelmisto, yksi tallennusmedia

- verkkoon aiheutuva kuormitus varmistuksen aikana
- hankintahinta.

Kasvavat tietomäärät asettavat varmistus- ja palautusjärjestelmille erilaisia vaatimuksia. Monessa yrityksessä sovellukset ovat käytössä 24 tuntia vuorokaudessa vuoden jokaisena päivänä. Tästä johtuen varmistus- ja palautusjärjestelmässä on oltava kyky ottaa varmistukset on-line -tilassa, jotta käyttöä ei tarvitse keskeyttää varmistuksien ajaksi. Järjestelmän pitää suoriutua tehtävästään sallitussa ajassa, minkä ansiosta skaalattavuusominaisuus on tärkeä huomioon otettava seikka. Varmistusjärjestelmä tarvitsee joustavat hallintyökalut, joiden avulla järjestelmää voidaan hallita keskitetysti, etäyhteyden kautta tai osana suurempaa varmistuskokonaisuutta.

On siis useita erilaisia tapoja toteuttaa varmistus, mutta kaikissa vaihtoehdoissa kannattaa ottaa huomioon: miten varmistukset otetaan, kuinka nopeasti on suoriuduttava varmistuksesta, palautuksesta ja paljonko tietoa on arkistoitava. Valittavista laitekokonaisuuksista olisi vielä löydettävä sopiva tasapaino hinnan ja suoristuskyvyn välillä. Seuraavaksi on esitelty yleisimpiä varmistusohjelmistoja.

3.1 Windows Backup tool

Windows Backup (NTBackup.exe) on varmistus- ja palautustyökalu, joka tulee Windowsin mukana. Backup -työkalu tukee useita erilaisia varmistustapoja: normaali (normal), kopiointi (copy),

inkrementaalinen (incremental) ja differentiaalinen (differential). Kuten jo aikaisemmin on todettu, Actice Directory varmistetaan osana System State -tilaa. Näin ollen ainoa käytettävä varmistustyyppi on normaali. Backup -työkalu merkitsee jokaisen tiedoston varmistettavaksi on-line tiedostoksi, minkä ansiosta tiedoston arkistoattribuutti tyhjenee. ([3@][Microsoft])

Windows Backup -työkalu on hyvä vaihtoehto pienille yrityksille, joissa varmistettava ympäristö koostuu vain muutamista palvelimista. Backup -työkalun kanssa voidaan käyttää Windowsin Ntdsutil nimistä komentorivityökalua, jolla saadaan määriteltyä tarkemmin Backup -työkalun asetuksia. ([4@][Microsoft])

3.2 VERITAS Backup Exec

Backup Exec -ohjelma tarjoaa kattavan, kustannustehokkaan ja sertifioidun varmistustyökalun nauha- tai levyvarmisteiselle Microsoft Windows -palvelinympäristölle. Helppokäyttöisen web-pohjaisen hallintatyökalun avulla ylläpitäjät voivat määritellä halutut varmistuskäytännöt kaikenkokoisissa yrityksissä tai organisaatioissa. ([5@][VERITAS Software]):

+ helppo kasvattaa organisaation koon mukaan
+ yksinkertainen hallita
+ vähentää hallinnallisia kuluja Windows -ympäristöissä
+ parantaa Windows -palveluiden saatavuutta verkossa
+ tarjoaa sertifioidun yhteensopivuuden Windows 2000 ja 2003 -palvelimien kanssa.

Backup Exec -ohjelma on suunniteltu pienentämään verkkoliikennettä ja maksimoimaan läpimeno suorituskykyä (troughput).

3.3 CA BrightStor ARCserve Backup ([6@][Computer Associates])

Computer Associatesin valmistama BrightStor ARCserve Backup on yksi tunnetuimmista varmistustyökaluista maailmassa. ARCserve tukee älykästä datahallintaa, jossa järjestelmäylläpitäjät voivat määritellä omat varmistuskäytännöt (Backup policy).

ARCserve tarjoaa tiedostovarmistusta monelle eri ympäristölle, kuten Microsoft Windows, NetWare, Linux ja Unix. Lukuisten optioiden ja ohjelmien avulla ARCserve saadaan optimoitua monel-

le eri ohjelmalle ja tietokannalle esim: Microsoft Exchange, Oracle, Microsoft SQL, MySQL, Informix, Lotus Notes, SAP R/3, Sybase ja Apache. ARCserve Backup tukee kaikentyyppisiä varmistusympäristöjä, mukaan lukien DAS (Direct-Attached-Storage), NAS (Network Attached Storage) ja SAN (Storage Area Networks).

ARCserve on myös erittäin skaalautuva, joten sitä voidaan käyttää yhden palvelimen ympäristöstä laajaan data center ympäristöön. Näin ollen tuote soveltuu kaikenkokoisissa yrityksissä tai organisaatioissa.

3.4 EMC Legato NetWorker ([7@][EMC])

Legato NetWorker on myyntiosuudella markkinajohtaja varmistus- ja palautusjärjestelmissä. NetWorker -ohjelma soveltuu heterogeenisiin ympäristöihin, joissa sen avointa ja skaalautuvaa arkkitehtuuria voidaan käyttää erilaisten järjestelmien suojaamiseen. Näitä järjestelmiä ovat Unix, Windows, OpenVMS, NetWare, Macintosh sekä virtuaaliset VMWare ja Microsoft Virtual Server 2005 systeemit.

NetWorkerilla voidaan suojata giga- ja teratavun kokoisia järjestelmiä käyttäen hyväksi LAN -, SAN - ja WAN -yhteyksiä. Varmistuslaitteet voivat olla yksittäisiä nauhureita, nauhakirjastoja tai levyohjaimia. Networkerin etuja ovat:

+ 10.1 TB/h jatkuva varmistus- ja 4.5 TB/h palautusnopeus
+ 1 TB tiedostotason varmistus 7 ja palautus 16 minuutissa
+ saumaton siirtyminen SMB:stä Enterprise -tason tuotteeseen
+ edistyneet kuormantasausominaisuudet.

Erilaisia varmennustuotteita on maailmassa satoja tai jopa tuhansia. Yrityksen tai organisaation tulee tarkastella ja vertailla, mikä sovellus parhaiten sopii omaan ympäristöön. Isojen ohjelmistotalojen sovellukset ovat yleensä kalliimpia, mutta rahalla saa myös vastinetta tuen, päivityksien ja koulutuksen muodossa. Monet ohjelmistot toimitetaan laitteiden mukana, jolloin yhteensopivuus on parempi ja testatumpi.

3.5 Nauhavarmistusmediat

Nauhat ovat edullinen tapa tiedon varmennukseen ja arkistointiin. Järjestelmän kapasiteetti on näennäisesti loputon, sillä tarvittaessa ostetaan vain uusia nauhoja. Yleisesti yrityksissä käytetään nauha-robotteja, missä järjestelmä vaihtaa nauhan asemaan ja suorittaa varmistuksen. Nauhoja kierrätetään robotissa, kunnes ne pitää vaihtaa uuteen, sillä esim. yksi DAT-nauha kestää noin 40 - 50 nauhoituskertaa. Alla on esitelty yleisimmät nauhamediat.

3.5.1 LTO ([8@][Ultrium)

Linear Tape-Open (LTO) on HP:n, IBM:n ja Seagaten alulle panema aloite, jossa haetaan ratkaisua pirstaloituneille nauhamarkkinoille. Kyseiset valmistajat näkivät tarpeen kehittää nauhateknologian, jossa ei olisi kompromisseja ja jonka kehityskäyrä olisi määritelty pitkälle tulevaisuuteen. LTO:n tarkoituksena on tarjota käyttäjille johtava nauhaformaatti toteutettuna todistettavasti toimivilla tekniikoilla.

LTO Ultrium formaatti on korkeakapasiteettinen ja yksikelainen LTO -teknologian ilmentymä. Se sopii parhaiten varmistukseen, palautukseen tai tiedon arkistoimiseen. Ultrium tarjoaa luotettavan ja toiminnallisen ratkaisun niin yksittäisiin tai automatisoituihinkin ympäristöihin. Ultriumia käytetään mieluiten ratkaisuissa, missä kapasiteettimäärä on tärkeämpi kuin nauhajärjestelmän nopeus.

Kolmannen sukupolven Ultrium -nauhassa on 800GB -tallennuskapasiteetti (2:1 pakkaus). Ultrium -nauhoja suunnitellaan jo sukupolvia eteenpäin. Näkyvissä on jo kuudennen sukupolven nauha, johon on mahdollista tallentaa jopa 6.4TB (2:1 -pakkauksella).

3.5.2 DLT/SDLT ([9@][DLT -tape)

Digital Linear Tape (DLT) on käytetyin varmistusmuoto maailmassa. DLT -nauhuri tallentaa tiedon raidoittain kelaamalla nauhaa edestakaisin. Nauhurissa on erilliset luku- ja kirjoituspäät, jotka mahdollistavat kirjoituksen tarkastamisen heti kirjoituksen

jälkeen. Kun nauhan loppu saavutetaan, sitä ei kelata alkuun, vaan nauha lähtee pyörimään toiseen suuntaan, jolloin luku- ja kirjoituspää on siirretty seuraavalle uralle. Tätä toistetaan, kunnes kaikki urat ovat täynnä.

DLT käyttää tallentamiseen metallioksidinauhoja. Keskimääräiseksi vikaantumisväliksi DLT -nauhurille on määritelty noin 80 000 käyttötuntia. Nauhat säilyvät oikein säilöttynä noin 30 vuotta. Tape Pass arvo kertoo, kuinka monta kertaa nauha voidaan lukea tai kirjoittaa päästä päähän. Yleisesti tämä arvo on 50 000 DLT-nauhoissa. Super Digital Linear Tape (SDLT) on DLT- nauhan uudempi versio. SDLT – nauhuri on 45 % nopeampi kuin tavallinen DLT ja sen kapasiteetti on jopa 320GB.

3.5.3 DDS ([10@][DLT -tape)

Digital Data Storage (DDS) on nauhaformaatti, jonka HP ja Sony kehittivät vuonna1989 datan varmistamiseen käyttäen hyväksi DAT -tekniikkaa (Digital Audio Tape). DDS formaatin nauhoja voidaan käyttää sekä DAT- tai DDS -nauhureilla.

DDS käyttää 4 mm:n kasettia, jossa on kaksi luku- ja kirjoituspäätä. Samaa tekniikkaa tallentamisessa käyttää myös videot. Lukupäät tarkistavat kirjoitetun datan. Jos virheitä ilmenee, kirjoituspäät kirjoittavat datan uudestaan. DDS -nauhureita on neljää eri tyyppiä.

1. DDS-1 tallentaa 2 GB pakkaamatonta dataa 120 minuutin nauhalle.

2. DDS-2 tallentaa 8 GB pakattua dataa 120 minuutin nauhalle.

3. DDS-3 tallentaa 24 GB dataa 125 minuutin nauhalle.

4. DDS-4 on uusin DDS -nauhuri, joka pystyy tallentamaan 40 GB 125 minuutin nauhalle.

DDS -nauha pitää vaihtaa 2000 nauhoituskerran jälkeen. Lisäksi suositellaan, että nauhuri puhdistetaan vuorokauden välein puhdistusnauhalla, joka vaihdetaan 30 käyttökerran jälkeen. DDS -nauhureille luvataan ainakin 10 vuoden käyttöikä.

3.6 Palvelimen vikasietoisuus

Active Directory vaatii palvelimelta paljon ja näin ollen sen pitää toimia varmasti ja olla kaiken lisäksi vikasietoinen. Kun Active Directory asennetaan palvelimeen, järjestelmäylläpitäjän on hyvä ottaa huomioon seuraavia seikkoja, joiden avulla voidaan välttää ongelmatilanteita palvelimen näkökulmasta:

+ riittävät resurssit
+ häiriötön virransyöttö - UPS
+ hot Swap -komponentit
+ palvelimen fyysinen sijoittaminen
+ klusterointi
+ levyjärjestelmä – Raid.

3.6.1 Riittävät resurssit

Kun yritys tai yhteisö hankkii uutta palvelinta, vaihtoehtoja on paljon. Markkinoilla on monia ”pelureita”, jotka ylistävät tuotteitaan erilaisilla ominaisuuksilla ja takuilla. Monesti palvelimet voivat tulla ylläpito- tai ulkoistamissopimuksen mukana, jolloin palvelun tuottaja yleensä käyttää itse hyväksi havaittuja laitevalmistajia. Jos laite kuitenkin hankitaan itse, voi sen mitoittaminen olla välillä hankalaa.

Pieneen ympäristöön ostetaan yleensä vain yksi palvelin, joka hoitaa kaikkia ohjauspalvelimen rooleja. Nyrkkisääntönä voidaan pitää, että Microsoftin omat vähimmäisvaatimukset kerrotaan moninkertaisesti, jotta päästään sellaiseen kokoonpanoon, mikä toimisi. Kaikkien isojen laitevalmistajien uudet palvelimet ovat kuitenkin jo riittävän tehokkaita pieniin ympäristöihin. Hintaa lisäävät komponenttien variaatiot, joihin palataan myöhemmin.

3.6.2 UPS ([11@][Tietoturva])

Häiriötön virransyöttö, joka tunnetaan paremmin nimellä UPS (Uninterruptible Power Source), pyrkii takaamaan katkeamattoman virransyötön tietokoneeseen. UPS ei ole siis ohjelma, vaan laite, jonka tehtävänä on suojella tietokoneen herkkiä laiteosia ja arvokasta tietoa. UPS -laite sijoitetaan virtalähteen (pistorasia) ja tietokoneen välille. Riippuen UPS:n koosta ja akun kestosta, voidaan se kytkeä ohjelmallisesti tietokoneeseen, jolloin sähkökat-

koksen sattuessa UPS antaa virtaa koneelle esim. 20 minuutin ajan, jonka jälkeen keskeneräiset työt tallennetaan ja ohjelma sammuttaa koneen turvallisesti, jos virransyöttö ei ole palautunut siihen mennessä.

Virransyötön takaamisen lisäksi UPS turvaa konetta erilaisilta vahingollisilta virtapiikeiltä, joita voi esiintyä sähköverkossa:

- ukonilma
- kova kylmyys (sähköverkko ylikuormittuu)
- myrsky, lumi (puut katkovat sähkölinjoja)
- inhimilliset syyt (Kaivuri törmää muuntajatolppaan).

Isommissa yrityksissä virransyöttö on vielä taattu järeillä diesel- tai bensiinikäyttöisillä generaattoreilla, jotka tuottavat sähköä koko yrityksen tarpeisiin ongelmatilanteiden sattuessa.

3.6.3 Hot Swap

Hot Swap tarkoittaa suomeksi ”lennossa vaihdettava”. Nykyisissä uusissa yrityspalvelimissa käytetään sellaisia komponentteja, jotka voidaan vaihtaa käytön aikana. Yleisimmät hot-swap -komponentit ovat virtalähde ja kiintolevyt. Kalliimmissa malleissa voidaan vaihtaa myös muita komponentteja, kuten tuulettimia.

Esimerkki palvelimesta:

HP ProLiant DL380 G4 (HP:n mukaan maailman myydyin palvelin) [12@][HP]

- Intel Xeon 3,20 GHz
- 6 Gt muistia
- viisi käytön aikana vaihdettavaa kiintolevyasemaa ja yksi käytön aikana vaihdettava DAT-nauha -asema
- käytön aikana vaihdettavat vikasietoiset tuulettimet ja virtalähteet
- Gigabit ethernet -verkkokortti
- 3 vuoden takuu osille ja työlle, huolto asiakkaan tiloissa 3 vuoden ajan.

Isommat laitevalmistajat pystyvät antamaan kattavampia takuu- ja vasteaikoja rikkoutuneille laitteille tai osille. Kriittisissä ympäristöissä tällainen lisäarvo on todella hyödyllinen, ja siitä kannattaa myös maksaa, jos rikkoutunut osa toimitetaan tilalle alle kolmessa tunnissa vikailmoituksesta.

3.6.4 Palvelimen sijoittaminen

Palvelimen sijoittaminen on myös tärkeä tekijä minimoitaessa riskitekijöitä. Pahimmillaan palvelin voi olla pölyttymässä ja potkittavana työpöydän alla, jossa se lojuu vuodesta toiseen kunnes jotain tapahtuu! Pienissä yrityksissä ei ole järkeä rakentaa kallista palvelinhuonetta. Yksinkertainen ja toimiva ratkaisu on hankkia yksittäinen palvelinkaappi. Tällaiseen yleiskaappiin saadaan helposti asennettua kaikenlaiset palvelintyypit, kaapelointi ja virransyöttö saadaan tuotua runkoprofiilin sisällä. Jos laitteiden määrä kasvaa voidaan kaappeja modulaarisesti parannella vastaamaan yrityksen tarpeita.

Palveluntarjoajien ja isojen yrityksien palvelintilat ovat kuitenkin tarkasti suunniteltuja ja hallittuja tiloja. Tässä muutamia konesalien ominaisuuksia [13@][Song Networks]:

- kahdennettu pääsähkönsyöttö
- kahdennettu UPS -järjestelmä ja dieselgeneraattori
- varmennettu ilmastointi
- varmennettu operaattoritason tietoliikenneyhteydet
- kulunvalvonta
- kameravalvonta
- palosuojaus rakennusstandardin mukaisesti
- automaattinen Ingren -kaasupohjainen sammutusjärjestelmä
- murtosuojattu
- emp -pulssisuojaus (Faradayn häkki)
- kaapelinvientijärjestelmä
- valvonta 24 h/vrk 7 päivänä viikossa.

3.6.5 Klusterointi

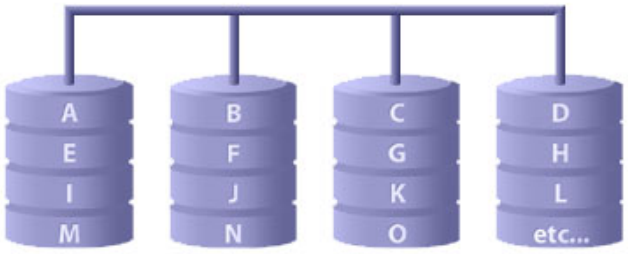
Palvelinklusteri on ryhmä itsenäisiä, solmuiksi kutsuttuja palvelimia, joita ylläpidetään yhdessä. Klusteroinnin tavoite on saavuttaa erittäin hyvä tietojen ja ohjelmien käytettävyys. Klusterointi lyhentää seisokkiaikoja ja pienentää näin kustannuksia, koska järjestelmä toimii, vaikka jokin klusterin järjestelmistä kaatuisi. Palvelinklusteria käyttäen yritykset voivat pienentää laitteistokustannuksia, koska klusteri muodostetaan edullisimmista palvelimista. Kehittyneiden kuormatasaus ominaisuuksien avulla palvelimet saadaan mukautumaan käyttäjien vaatimuksiin tarpeen mukaan. Jos jokin palvelin kaatuu tai sammutetaan huoltoa varten, klusteri osaa ohjata asiakkaiden pyynnöt muihin saatavilla

oleviin palvelimiin. Näin verkon palvelut ovat jatkuvasti käytettävissä. [14@][Microsoft]

3.6.6 RAID -levyjärjestelmä

RAID (Redundant Array of Inexpensive Disks) tarkoittaa mahdollisuutta käyttää useita kiintolevyjä yhdistettynä yhdeksi levyjärjestelmäksi. Näin saadaan aikaan erittäin vikasietoinen levyjärjestelmä verrattuna yksittäiseen kiintolevyyn. Raid arrayssa eli levypakassa olevat yksittäiset kiintolevyt eivät näy käyttäjille, vaan ne näkyvät yhtenä, virtuaalisena kiintolevynä, jota voidaan käsitellä normaaliin tapaan. Valtaosassa RAID -järjestelmistä käyttää kalliimpia SCSI–kovalevyjä, mutta tavallisiin kotikoneissa käytettäviin ATA -kovalevyihinkin löytyy RAID -ratkaisuja. RAID:t määritellään eri tasoille, joilla kaikilla on omat käyttötarkoitukset. Tässä yleisimmät tasot [15@][MB]:

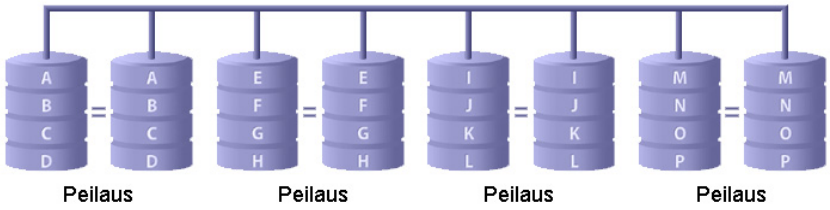
- Ensimmäinen taso on RAID 0 (Kuva 4), josta käytetään myös nimitystä striping. Tällä tasolla tieto kirjoitetaan pala kerrallaan kahdelle tai useammalle kiintolevylle lomitetusti. Kapasiteetti on pakan pienimmän levyn kapasiteetti kerrottuna kiintolevyjen lukumäärällä. Ideana stripingissa on, että datan takaisin lukeminen keskusmuistiin on nopeampaa, kun se tapahtuu useammalta levyltä vuorotellen. RAID 0:a ei pidetä todellisena RAID:na, sillä se ei ole vikasietoinen. Yhden levyn rikkoutuminen johtaa siihen, että koko data menetetään. Tästä syystä sitä ei saisi käyttää kriittisissä ympäristöissä. [16@][AC&NC]



Kuva 4. RAID 0 [16@][AC&NC]

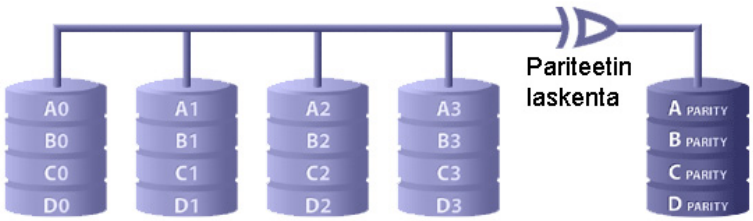
- RAID 1 (Kuva 5) tunnetaan myös nimellä mirroring eli peilaus. Tällä tasolla tieto kirjoitetaan yhtä aikaa kahdelle tai useammalle levylle. Kiintolevyn hajotessa raid -ohjain siirtyy lukemaan automaattisesti toista levyä, eikä käyttöön tule katkosta. Levypakan tallennuskapasiteetti on sama kuin pakan pienimmän kiintolevyn kapasiteetti. RAID 1:ssä uhrataan samankokoisia kiintolevyjä käytettäessä puolet tallennuskapasiteetista, mutta tuloksena saadaan

erittäin hyvä fyysinen vikasietoisuus ja katkeamaton toiminta. [16@][AC&NC]



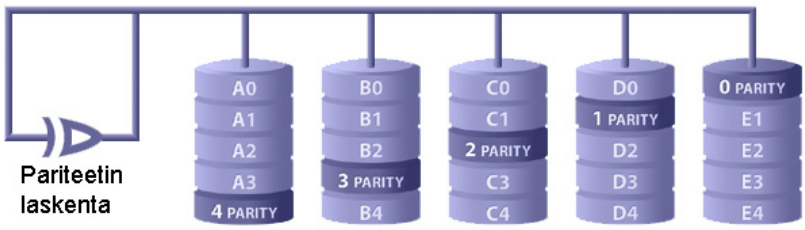
Kuva 5. RAID 1[16@][AC&NC]

- RAID 3 (Kuva 6) toimii kuten taso nolla, missä tieto jaetaan useammalle eri levylle, mutta yhtä levyä käytetään tarkistusbittien tallentamiseen. Yksittäisen levyn hajotessa voidaan tieto palauttaa tarkistusbittien avulla. Järjestelmän kapasiteetti on kiintolevyjen summa vähennettynä yhden kiintolevyn koolla. [16@][AC&NC]



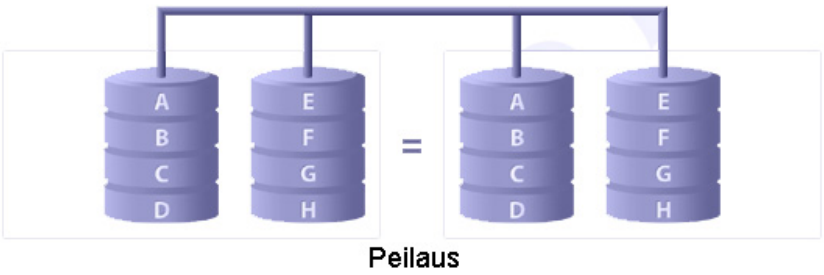
Kuva 6. RAID 3[16@][AC&NC]

- RAID 5 (Kuva 7) vaatii vähintään kolme kiintolevyä toimiakseen. RAID 0:n tyyliin kaksi kiintolevyä sisältää varsinaisen tiedon ja yhdelle levylle kirjoitetaan pariteettitarkistustieto. RAID 5 kestää yhden levyn hajoamisen. RAID 5 on ylivoimaisesti käytetyin RAID taso. Kyseisellä järjestelyllä saadaan aikaan erittäin suuri lukunopeus ja keskinkertainen kirjoitusnopeus. Yleisimpiä käyttökohteita ovat sovellus- ja tiedostopalvelimet.



Kuva 7. RAID 5 [16@][AC&NC]

- RAID 0+1 (Kuva 8) eli mirrored stripping yhdistää 0- ja 1-tasojen parhaat puolet, jos käytettävissä on vähintään neljä kiintolevyä. Kahdelle eri levylle kirjoitettu tieto peilataan automaattisesti kahdelle muulle levylle. RAID 0+1 on melko kallis toteuttaa, sillä levyjä ”tuhlataan”. [16@][AC&NC]



Kuva 8. RAID 0+1 [16@][AC&NC]

4 Active Directoryn katastrofitilanteesta toipuminen

Aiemmissa kappaleissa on käyty läpi Active Directorya yleensä ja sen tärkeimpiä palveluita ja palvelinrooleja. Lisäksi on tarkasteltu, mitä Active Directorysta pitää varmistaa ja millä sekä mikä edesauttaa parempaan vikasietoisuuteen laitteistonäkökulmasta. Varmistaminen sekä vikasietoisuus ovat täysin eri asioita, jotka eivät korvaa toisiaan, vaan yhdessä muodostavat edellytykset toimivaan ympäristöön. Kun käsitellään Active Directoryn katastrofitilannetta, pitää aluksi määritellä, minkä tyyppisestä katastrofista on kyse. Työssä käydään läpi kahta ongelman aiheuttajaa ja niihin soveltuvia ratkaisuja.

1. Tietokannan korruptoituminen

Tietokanta voi korruptoitua seuraavista syistä:

- Kiintolevy korruptoituu, kun virta katkeaa kesken kirjoituksen.
- Ohjauspalvelin tai sen jokin osa hajoaa fyysisesti.
- Ohjelmisto vika tai virus estää Active Directorya toimimasta.

2. Inhimillinen erehdys

Inhimillinen erehdys on myös erittäin suuri riskitekijä, kun järjestelmäylläpitäjät käyttävät Active Directoryn työkaluja, esim. ”Users and Computers”. Kyseisellä työkalulla voidaan luoda/poistaa käyttäjiä, tietokoneita, ryhmiä ja organisaatioyksiköitä (OU). Jos käyttäjä vahingossa tai tietämättään siirtää organisaatioyksikön pois ja tämä tieto replikoidaan kaikille metsän ohjauskoneille, pitää olla tapa saada Active Directory palautettua toimivaan kuntoon. (Active Directory Disaster Recovery White Paper 2000: 12.)

4.1 Active Directoryn palauttaminen

Ohjauspalvelimen palauttaminen toimintakuntoon uudelleenasennuksen kautta voi toimia ainoastaan, jos toimialueella sijaitsee toinen toimiva ohjauspalvelin. Tällöin System State tilaa ei palauteta varmuuskopiolta, vaan Windows -käyttöjärjestelmä ja Active Directory -palvelu asennetaan koneeseen uudestaan. Tämän jälkeen järjestelmä nostetaan (DCPROMO) takaisin ohjauspalvelimeksi siihen toimialueeseen, missä se oli ennen vikaantumista. Tämän toiminnan aikana toimialueen muut ohjaus-

palvelimet replikoivat ajan tasalla olevan kopion Active Directoryn tietokannasta takaisin uudelleenasennetulle ohjauspalvelimelle. Kyseistä tapaa suositellaan käytettäväksi ainoastaan silloin, kun ei ole käytettävissä hyvää varmuuskopiota ohjauspalvelimesta. (Active Directory Disaster Recovery White Paper 2000: 16.)

Tärkeimpiä huomioonotettavia seikkoja käytettäessä ohjauspalvelimen palauttamista replikoinnin avulla on verkon siirtokapasiteetti. Tarvittava kaistanleveys on suoraan riippuvainen siitä, kuinka suuri Active Directoryn tietokanta on ja kuinka nopeasti ohjauspalvelimen pitää olla toimintakunnossa. Nykyisissä yrityksissä on laajasti käytössä jo nopeat 100Megan tai jopa Gigabitin lähiverkkoyhteydet. Tällaisten nopeiden yhteyksien avulla kaistanleveys ei ole niin suuri este kun, puhutaan puhtaasta replikointiliikenteestä. Jos kuitenkin palautettava ohjauspalvelin on hitaan yhteyden takana ja jos Active Directoryn tietokannan koko on useita Gigatavuja voi replikointi viedä runsaasti aikaa. (Active Directory Disaster Recovery White Paper 2000: 16.)

Yhteenveto ohjauspalvelimen palauttamisesta uudelleenasentamisen ja replikoinnin avulla:

- Toimialueella pitää olla vähintään yksi toimiva ohjauspalvelin.
- Poistetaan vioittuneen ohjauspalvelimen objekti AD:sta.
- Varmistetaan ettei ongelma johtunut palvelimen fyysisestä laitteistoviasta.
- Asenna Windows Server -käyttöjärjestelmä uudestaan.
- Nosta kyseinen kone ohjauspalvelimeksi toimialueeseen.
- Tarkista Active directoryn toimivuus.

(Active Directory Disaster Recovery White Paper 2000: 16.)

4.2 Ohjauspalvelimen palauttaminen varmuuskopion avulla

Kyseinen tapa perustuu pääasiassa viimeksi otettuun hyvään varmistukseen ennen ongelmatilannetta. Palautusprosessi voidaan käynnistää joko Windowsin oman tai kolmannen osapuolen palautustyökalun avulla, niin kuin luvussa 3 kerrotaan. Palautusprosessi palauttaa ohjauspalvelimen siihen tilaan, kun se oli ennen varmistuksen ottamista. Tämän jälkeen se saa päivitetyn, ajan tasalla olevan Active Directory -tietokannan itselleen replikointikumppanin(en) avulla.

Tehtäessä ohjauspalvelimen palautus varmuuskopion avulla on olemassa vielä kaksi vaihtoehtoa:

- Ei-määrävä palautus (Non-Authorative Restore)
- Määräävä palautus (Authorative Restore)

Nämä kaksi metodia antavat järjestelmäylläpitäjälle mahdollisuuden manipuloida kahta tärkeää System State -tilan komponenttia Active Directorya ja SYSVOL:ia palautuksen aikana. Vaikka nämä kyseiset komponentit palautetaan yhdessä, esitellään ne kuitenkin erikseen. (Active Directory Disaster Recovery White Paper 2000: 19.)

4.2.1 Ei-määräävä palautus

Active Directory

Active Directoryn ei-määräävä palautus (Non-Authorative Restore) palauttaa ohjauspalvelimen tilaan, jossa se oli otettaessa varmistusta. Tämän jälkeen se sallii normaalin replikointiliikenteen, jolloin kaikki varmuuskopioinnin ottamisen jälkeen tapahtuneet muutokset kopioituvat tämän tilan päälle. Kun System State -tila on palautettu, ohjauspalvelin lähettää kyselyitä replikointikumppaneilleen. Kyseiset kumppanit replikoivat kaikki muutokset palautetulle ohjauspalvelimelle ja näin varmistavat, että ohjauspalvelimella on tarkka ja ajantasainen kopio Active Directoryn tietokannasta. (Kivimäki 2004: 1003)

Ei-määräävä palautus on oletusarvoinen tapa palauttaa Active Directory. Tästä johtuen sitä käytetään useimmissa tilanteissa, jotka ovat aiheutuneet Active Directoryn tietojen häviämisestä tai korruptoitumisesta tavalla, joista on mainittu kappaleen alussa. Jotta ei-määräävää palautusta voidaan käyttää, pitää ohjauspalvelimen voida käynnistyä Directory-Services Restore -tilassa. (Active Directory Disaster Recovery White Paper 2000: 20)

SYSVOL

Kun SYSVOL palautetaan ei-määräävän palautuksen avulla, palautetulla ohjauspalvelimella olevaa SYSVOL:n paikallista kopiota verrataan replikointikumppaneilla olevaan kopioon. Kun ohjauspalvelin käynnistyy uudestaan, se ottaa yhteyden muihin replikointikumppaneihinsa, vertaa SYSVOL -tietoja ja replikoi kaikki tarvittavat muutokset. Näin palautettu ohjauspalvelin on jälleen ajan tasalla toimialueen muiden ohjauspalvelimien kanssa. SYSVOL:n ei-määräävä palautus on suositeltavaa, jos toimialueella on vähintään yksi toimiva ohjauspalvelin. Kyseinen tapa palauttaa SYSVOL on oletusarvoinen ja se tapahtuu automaatti-

sesti suoritettaessa Active Directoryn ei-määräävä palautus. (Active Directory Disaster Recovery White Paper 2000: 20)

Jos toimialueella ei ole yhtään toimivaa ohjauspalvelinta kannattaa suorittaa SYSVOL:n primary restore -palautus. Primary restore -palautus luo uuden tiedostojen replikointipalvelutietokannan (File Replication Service, FRS) lataamalla paikallisen ohjauspalvelimen SYSVOL:ssa olevat tiedot. Tämä tapa on sama kuin ei-määräävä palautus, paitsi että SYSVOL merkitään primääriksi. (Active Directory Disaster Recovery White Paper 2000: 20)

4.2.2 Määräävä palautus

Active Directory

Määräävä palautus (Authorative Restore) on lisäys oletuksena olevaan ei-määräävään palautusprosessiin. Ei-määräävän palautuksen työvaiheiden pitää olla suoritettuna, ennen kuin määräävä palautus voidaan suorittaa.

Pääerona on, että määräävä palautus pystyy kasvattamaan koko hakemiston kaikkien objektien, alahaaran kaikkien objektien tai yksittäisen objektin (olettaen, että kyseessä on lehtiobjekti) attribuuttien versionumeron, jotta siitä tulee hakemistossa määräävä. Tässä palautetaan pienin mahdollinen yksikkö; ei esimerkiksi palauteta koko hakemistoa, kun halutaan palauttaa vain yksittäinen alahaara. Active Directory Disaster Recovery White Paper 2000: 20 - 21.)

Toimintaan palautunut ohjauspalvelin ottaa yhteyden replikointikumppaneihinsa aivan kuten ei-määräävän palautuksenkin yhteydessä ja ottaa selville, mitä muutoksia viimeisen varmuuskopion jälkeen on tapahtunut. Koska määräämiksi haluttujen objektien attribuuttien versionumerot ovat korkeammat kuin replikointikumppaneilla olemassa olevien attribuuttien versionumerot, palautetulla ohjauspalvelimella olevat objektit näyttävät olevan uudempia, ja siksi ne replikoituvat muihin ympäristön ohjauspalvelimiin. (Kivimäki 2004: 1004.)

Toisin kuin ei-määräävä palautus, määräävä palautus edellyttää erillisen Ntdsutil.exe -työkalun käyttöä (Esim. liite 1). Millään muulla varmuuskopiointiapuohjelmalla ei voida tehdä kyseistä Active Directory -palautusta. Määräävä palautus suoritetaan inhimillisen virheen aiheuttamassa virhetilanteessa, mm. silloin, kun järjestelmäylläpitäjä vahingossa poistaa useita objekteja ja muutos on replikoitunut muille toimialueen ohjauspalvelimille eikä objekteja voida helposti luoda uudelleen. Määräävää palau-

tusta varten ohjauspalvelin pitää käynnistää Directory Services Restore -tilassa. Määräävä palautus ei päällekirjoita uusia objekteja, jotka on luotu varmuuskopion ottamisen jälkeen. Määräävästi voidaan palauttaa vain konfiguraatioon ja toimialueiden nimikontekstiin liittyviä objekteja. Toiminto ei tue nimeämiskontekstien määräävää palautusta (Actice Directory kaava (Schema)). (Active Directory Disaster Recovery White Paper 2000: 21.)

SYSVOL

Kun SYSVOL palautetaan määräävästi, se määrittelee automaattisesti sen, että varmuuskopiolta palautettu SYSVOL on määräävä toimialueessa. Tarvittavien asetusten jälkeen (kts. liite 1) Active Directory merkitsee paikallisen SYSVOL:in määräävästi (Autohorative) ja se replikoidaan toimialueen muille ohjauspalvelimille. Samaan tapaan kuin Active Directoryn määräävä palautus, käytetään tätä tapaa inhimillisten virheiden korjaamiseen, jotka ovat replikoituneet muille ohjauspalvelimille. Esimerkiksi ylläpitäjä on tuhonnut Group Policy -objektin, joka sijaitsee SYSVOL:n alla. (Active Directory Disaster Recovery White Paper 2000: 21.)

4.3 Varmuuskopion palauttaminen eri palvelimeen

On mahdollista palauttaa ohjauspalvelin fyysisesti erilaiseen palvelimeen kuin alkuperäinen. Kuitenkin on asioita jotka pitää ottaa huomioon ennen tällaisen tehtävän aloittamista (Active Directory Disaster Recovery White Paper 2000: 21 - 23):

- Hal.dll tiedostoa ei varmisteta System State -tilan yhteydessä, vaan ainoastaan Kernel32.dll. Tästä johtuen, jos yritetään palauttaa varmuuskopio koneeseen, joka tarvitsee erilaisen Hall.dll -tiedoston tukeakseen järjestelmäkokoonpanoa, tulee yhteensopivuusongelmia. Ainoa tapa on kopioida vanhasta koneesta Hall -tiedosto ja asentaa se uuteen koneeseen. Rajoituksena on kuitenkin se, että uusi kone käyttää ainoastaan yhtä prosessoria.

- Varmista, että boot.ini -tiedosto on sopiva uuden laitekokoonpanon kanssa, muuten voi tulla ongelmia laitteen käynnistyksessä.

- Jos uudessa laitekokoonpanossa on erilainen näytönohjain tai verkkokortti, tulee näiden laiteajurit poistaa. Kun kone

käynnistetään palautuksen jälkeen uudestaan, hoitaa Windowsin Plug and Play -toiminto niiden konfiguroinnin.

4.4 Vaikutus ryhmäjäsenyyteen (Group membership)

Määräävässä palautuksessa on olemassa riski ryhmäjäsenyyksiin liittyvien tietojen menettämisestä. Koska ryhmäjäsenyys on monesta arvosta koostuva attribuutti ja koska Active Directory käsittelee linkkejä, taaksepäin osoittavia linkkejä ja poistoja tietyllä tavalla, määräävä palautus voi ryhmäjäsenyyden kannalta tuottaa eri tuloksia. Tulokset riippuvat siitä, mitkä objektit replikoituvat ensimmäisenä määräävän palautuksen jälkeen: käyttäjäobjekti vai ryhmäobjekti. (Active Directory Disaster Recovery White Paper 2000: 23 - 24.)

Jos käyttäjän käyttäjätilin poiston kumoaminen replikoituu ensimmäisenä, sekä ryhmän (sisältämät jäsenet) että (ryhmän, joihin käyttäjä kuuluu) ryhmäjäsenyystiedot tallentuvat oikein. Jos ryhmän poiston kumoaminen replikoituu ensimmäisenä, replikointikumppanit jättävät (paikallisesti) poistetun käyttäjän lisäyksen pois ryhmäjäsenyydestä. Ainoana poikkeuksena on käyttäjän ensisijainen ryhmä, joka tallentuu oikein sekä käyttäjä- että ryhmäviittauksen mukaan. (Kivimäki 2004: 1005.)

Operaattori ei voi hallita objektien replikointijärjestystä määräävän palautuksen jälkeen. Jos tällä on vaikutusta ympäristön toimintaan, ainoa mahdollisuus on muuttaa vikaantuneiden ryhmien ryhmäjäsenyysattribuuttia sillä ohjauspalvelimella, jossa määräävä palautus on tehty. (Active Directory Disaster Recovery White Paper 2000: 23 - 24.)

Ongelma ei aiheudu palautetun tiedon yhtenäisyydestä vaan tavasta, jolla tiedot replikoituvat. Järjestelmäylläpitäjät voivat ohjauspalvelinta tarkastelemalla havaita, miltä hakemiston tulee näyttää ja replikoida täsmälliset hakemistoa koskevat tiedot muille toimialueiden ohjauspalvelimille. Paras tapa on lisätä väliaikaisesti uusi käyttäjä ja sitten poistaa se jokaisesta ryhmästä, jota määräävä palautus koski. Palautus koskee ryhmää, jos se on joko määräävästi palautettu tai jos palautuksen yhteydessä on palautettu ryhmän jäseniä, joilla kyseinen ryhmä ei ole määriteltynä ensisijaiseksi ryhmäksi. (Active Directory Disaster Recovery White Paper 2000: 24.)

Tällä tavoin operaattori pakottaa oikeat ryhmäjäsenyyttä koskevat tiedot replikoitumaan lähteenä toimivalta ohjauspalvelimelta (ohjauspalvelin, jossa on suoritettu alkuperäinen määräävä pa-

lautus) ja ryhmäjäsenyyttä koskevat tiedot päivittyvät ohjauspalvelimen replikointikumppaneille. Päivitetyissä objekteissa on oikeat tiedot ryhmäjäsenyyksistä ja oikeat tiedot näkyvät myös palautettujen käyttäjäobjektien ominaisuuksien Member of -välilehdessä. (Active Directory Disaster Recovery White Paper 2000: 24.)

Jos palautus tehdään väärin, virheelliset jäsenyystiedot voivat korruptoida hakemiston tarkan version, joka sijaitsi ohjauspalvelimella palautusta suorittaessa. Jos hakemiston tarkka versio korruptoituu, ryhmäjäsenyys pitää joko päivittää manuaalisesti tai objektit pitää palauttaa toisen määräävän palautuksen avulla verinc -valitsinta käyttäen ja suorittaa toimintosarja uudelleen. (Kivimäki 2004: 1006.)

4.5 Vaikutus luottosuhteisiin ja tietokonetileihin

Windows 2000/2003 neuvottelee luottosuhteet (Trust) ja tietokonetilien salasanat tietyin väliajoin. Kun suoritetaan määräävän palautus, voidaan palauttaa aikaisemmin käytettyjä salasanoja Active Directoryn luottosuhteita ja tietokonetilejä ylläpitäville objekteille. Luottosuhteisiin tulevat muutokset voivat vaikuttaa muiden toimialueiden ohjauspalvelinten väliseen kommunikointiin ja aiheuttaa käyttöoikeuksiin liittyviä virhetilanteita, kun käyttäjät yrittävät päästä käyttämään muilla toimialueilla olevia resursseja. Tämä voidaan korjata poistamalla NTLM-luottosuhteet Windows 2000/2003- tai Windows NT 4.0 -toimialueiden kanssa ja luomalla ne uudestaan. (Active Directory Disaster Recovery White Paper 2000: 24 - 25.)

Tietokonetilien salasanoihin tulevat muutokset voivat vaikuttaa liikenteeseen toimialueen jäsenenä olevan työaseman tai palvelimen ja ohjauspalvelimen välillä. Virheellinen tietokonetili voi aiheuttaa Windows NT –tai Windows 2000 –tietokoneiden käyttäjille autentikointiongelmia. (Active Directory Disaster Recovery White Paper 2000: 24.)

4.6 Global Catalog -palvelimen palauttaminen

Global Catalog -palvelimen palauttaminen voi tapahtua kahdella tavalla:

+ palauttaminen varmuuskopiolta
+ luomalla uusi korvaavan Global Catolog -palvelin

Varmuuskopio on ainoa tapa saada Global Catalog -palvelin palautettua automaattisesti toimivaan tilaan, palvelimeksi joka on ollut varmistuksen ottamisen aikaan Global Catalog -palvelin. Ohjauspalvelimen palauttaminen uudelleen asentamalla ei automaattisesti palauta Global Catalog -palvelimen roolia. Palauttaminen varmuuskopiolta vaatii enemmän aikaa kuin sellaisen ohjauspalvelimen, jossa ei ole Global Catalog -roolia. Global Catalog -palvelimia voi olla useita, joten järjestelmäylläpitäjät voivat asentaa uuden Global Catalog -palvelimen, jos näyttää siltä, että palautus aiheuttaa pidemmän käyttökatkoksen. Useiden Global Catalog -palvelimien konfigurointi lisää järjestelmän käytettävyyttä, mutta samalla se lisää replikointiliikennettä sekä tietokannan kokoa. Jos vikaantunut Global Catalog -palvelin asennetaan uudelleen ja säilytetään sen rooli, kannattaa harkita muiden sellaisten Global Catalog -palvelinten poistoa, jotka on mahdollisesti konfiguroitu käyttökatkon aikana. (Kivimäki 2004: 1008)

4.7 Operations master -tietokoneen palauttaminen

Kun Operations Master -roolin omaava palvelin on vikatilassa, voidaan rooli palauttaa seuraavasti:

+ Palautetaan vikaantunut Operations Master -palvelin varmuuskopiolta.

+ Kaapataan (seizing) rooli toiselle ohjauspalvelimelle. Tämä tehdään ainoastaan siinä tapauksessa, jos alkuperäistä roolin haltijaa ei palauteta. Kaappaaminen on järeämpi operaatio, jossa alkuperäinen roolin omaava palvelin ei tiedä, että rooli on siirretty. Kaappaamisessa saattaa seurata datan menetystä. (Active Directory Disaster Recovery White Paper 2000: 33.)

Uudelleen asennettu Operations Master -palvelin ei automaattisesti omaa kyseistä roolia. Uudelleen asennuksen jälkeen rooli voidaan siirtää hallitusti takaisin ohjauspalvelimelta, joka pitää kyseistä roolia kyseisellä hetkellä. Ohjauspalvelimen, joka ottaa roolin vastaan vikaantuneelta Operations Master palvelimelta, pitäisi olla samalla toimipaikalla (site) ja mahdollisesti vielä sen suora replikointipartneri. (Active Directory Disaster Recovery White Paper 2000: 23.)

4.8 Schema Master palvelimen palauttaminen

Schema Master -palvelimen ollessa vikatilassa Active Directoryn schemaan ei voida tehdä mitään päivityksiä. Useimmissa tuotantoympäristöissä kaavamuutosta tehdään kuitenkin todella harvaan ja tarvittaessa se valmistellaan hyvin. Jos halutaan kuitenkin kaapata kyseinen rooli, pitää miettiä, onko roolin poissaolo pitkäaikaista tai pysyvää. Ongelmatilanteiden välttämiseksi kannattaa kaappaus tehdä ainoastaan silloin, kun tiedetään, että alkuperäinen Schema Master -roolin omaava palvelin ei missään tapauksessa palaa enää aktiiviseksi. (Active Directory Disaster Recovery White Paper 2000: 34.)

Kuitenkin Schema Master -roolia tarvitaan yleensä niin harvoin, että on todennäköisesti järkevää palauttaa kyseinen roolin omaava ohjauspalvelin normaalisti. Jos kuitenkin Schema Master roolia tarvitaan välittömästi, pitää varmistaa, että vikaantunutta konetta ei koskaan tuoda takaisin Windows -verkkoon sellaisenaan. Tämän jälkeen roolin kaappaus voidaan toteuttaa. (Active Directory Disaster Recovery White Paper 2000: 35.)

4.9 Domain Naming Master -palvelimen palauttaminen

Domain Naming Master -palvelimen vikaantuminen ei myöskään häiritse tuotantoympäristöä pahasti, jollei vikaantumisen aikana tarvitse lisätä tai poistaa toimialuetta Active Directorysta. Domain Naming Master -roolin palauttamisessa ja kaappaamisessa on samat kriteerit kuin edellä käsitellyssä Schema Master -roolissa. (Active Directory Disaster Recovery White Paper 2000: 36.)

4.10 RID Master -palvelimen palauttaminen

RID Master -palvelimen vikaantuessa toimialueeseen ei voida Active Directoryn avulla luoda uusia käyttäjiä, ryhmiä tai tietokoneita. Kyseinen ongelma kuitenkin tulee eteen vasta silloin, kun kaikki ohjauspalvelimen yksittäiset RID -tunnisteet on käytetty loppuun sen varannosta. Kuitenkin jos käytössä on toimialue, jossa on viisi toimivaa ohjauspalvelinta, pitäisi teoriassa (5 x 500) 2500 RID -tunnistetta olla vielä jäljellä, kun kyseinen roolin omaava palvelin vikaantuu. Normaalissa Active Directory -ympäristössä tämän kyseisen varannon pitäisi riittää sen ajan, kun palvelin saadaan palautettua normaalisti. Jos kuitenkin tarvitaan suurempi määrä tunnisteita kuin on ohjauspalvelinten varannossa sillä hetkellä, voidaan roolin kaappaus toteuttaa. (Active Directory Disaster Recovery White Paper 2000: 37.)

RID Master -roolin kaappaamisen tarpeellisuutta pitää myös miettiä tarkoin, sillä on olemassa riski, että verkossa on identtisiä RID -tunnisteita. Jälleen pitää varmistaa, ettei roolin omannutta alkuperäistä ohjauspalvelinta tuoda takaisin verkkoon, jos kaappaaminen on toteutettu. (Active Directory Disaster Recovery White Paper 2000: 37.)

4.11 PDC Emulatorin palauttaminen

PDCE -roolin ollessa katastrofitilassa sekaympäristössä (mixed mode) ei voida hallinnoida NT 4.0 -toimialuetta kunnolla tai ollenkaan. NT -palvelin ilmoittaa, että se ei voi löytää toimialueen ohjauspalvelinta. Roolin puuttuminen aiheuttaa verkkoon kirjautumisongelmia Windows 2000/2003 -ympäristössä. Jos käyttäjä on unohtanut salasanansa ja järjestelmäylläpitäjä vaihtaa sen uuteen sellaisella ohjauspalvelimella, joka ei ota kirjautumisia vastaan, pitää käyttäjän odotella niin kauan kuin tieto on replikoitunut kirjautumista vastaanottavalle palvelimelle. (Active Directory Disaster Recovery White Paper 2000: 38.)

Toisaalta käyttäjän kirjautumista vastaanottava paikallinen ohjauspalvelin yrittää ottaa yhteyden PDCE -roolin omaavaan ohjauspalvelimeen tarkistaakseen, onko salasanaa muutettu viimeisen replikoinnin jälkeen. Tämä pyyntö ei onnistu, sillä PDCE ei ole toiminnassa. Tästä johtuen kyseinen autentikoiva ohjauspalvelin käyttää omaa paikallista kopiotaan Active Directorysta tarkastaakseen kirjautumisen oikeellisuuden, mutta sen oma tietokanta sisältää vielä tuon vanhan unohdetun salasanan. Ongelma voidaan kuitenkin kiertää tekemällä salasananvaihto autentikoi-

valla ohjauspalvelimella. (Active Directory Disaster Recovery White Paper 2000: 38.)

PDCE -rooli ei ole kriittinen, joten kaappaaminen voidaan tehdä helpommin perustein. Vikaantunutta PDCE -palvelinta ei tarvitse kokonaan asentaa uudestaan, että se voidaan tuoda takaisin verkkoon. Tästä johtuen roolin kaappaaminen on suositeltava käytäntö vikatilanteen sattuessa etenkin sekaympäristöissä. Ainoa tärkeä huomioon otettava seikka roolia kaapatessa on se, että jos toimitaan sekaympäristössä Windows NT 4.0 -palvelimien ollessa varaohjauspalvelimia, pitää sisäänrakennetut ryhmät synkronoida uuden PDCE palvelimen kanssa. (Active Directory Disaster Recovery White Paper 2000: 39.)

4.12 Infrastructure Master palvelimen palauttaminen

Infrastructure Master -palvelimen vikaantumisen aiheuttamat ongelmat ovat rajalliset. Se ei näy käyttäjille, vaan ainoastaan järjestelmäylläpitäjille, jos on tehty paljon ryhmien asetusten manipuloimista. Tyypillisesti tämä on käyttäjien lisäämistä tai uudelleennimeämistä. Vain harvoissa tapauksissa ympäristö ei tule toimeen sitä aikaan, kun roolin omaava ohjauspalvelin palautetaan normaalisti. Jos kuitenkin on ennustettavissa, että roolin osalta tulee pitkä käyttökatko, on kaappaus suositeltavaa. Roolia kaapatessa on vain varmistuttava siitä, että ohjauspalvelin, jolle rooli asennetaan, ei ole Global Catalog -palvelin, mutta omaa kuitenkin hyvät yhteydet kyseiseen palvelimeen. Ideaalisesti se sijaitsee samassa toimipaikassa (site). (Active Directory Disaster Recovery White Paper 2000: 41)

5 Yhteenveto

Active Directory on tehokas palvelu, jonka avulla yritykset ja yhteisöt voivat helposti hallita työasema- ja käyttäjäympäristöjään. Active Directory -palvelu on kuitenkin herkkä työkalu. Osaamaton ylläpitäjä voi saada suurtakin tuhoa aikaan muutamalla hiiren napsautuksella. Palveluihin kohdistuu myös paljon ulkoisia uhkia, kuten viruksia tai laitteistopuolen ongelmia. Työn tavoitteena on ollut tuoda esille se, kuinka tärkeää on, että yrityksissä on mietitty varasuunnitelmat mahdollisen katastrofitilanteen varalta. On ymmärrettävä, mitä Active Directoryn mahdollinen katastrofitilanne aiheuttaa yrityksen tietoverkolle ja mitä sen alhaallaoloaika maksaa.

Varasuunnitelman tekeminen pelkästään paperilla ei auta vielä mitään. Kuten armeijan kertausharjoituksissakin pitää ongelmatilanteita varten harjoitella konkreettisesti. Voiko yrityksen järjestelmävastaava todellakin nukkua yönsä rauhassa, jos Active Directorysta otettuja varmuuskopioita ei ole ikinä testattu? Miten on teidän yrityksenne laita? Nämä ovat kysymyksiä joita pitäisi lukijassa herätä ja joiden pitäisi toivottavasti aiheuttaa toimenpiteitä vielä kun on mahdollista. Muutaman kymmenen työaseman ympäristössä vikatilanne ei välttämättä ole paha, mutta entä jos virhe koskeekin 3000 työasemaa?

Active Directory -palvelut on suunniteltava huolellisesti sekä otettava heti alussa huomioon ne mahdolliset katastrofitilanteet ja muistettava dokumentoida. Jollei osata tehdä kaikkia asioita itse, kannattaa harkita palvelun ostamista ulkopuolisilta konsulteilta tai ulkoistaa ylläpito jollekin kolmannelle osapuolelle. On rajoitettava niiden henkilöiden määrää, joilla on oikeus ylläpitää Active Directory -palveluja, ja pidettävä huoli, että heitä koulutetaan jatkuvasti, sillä siihen menevä raha voi tuhatkertaistua hetkessä heidän tekemästään inhimillisestä virheestä. On myös huolehdittava, että palvelinten fyysiset edellytykset täyttyvät ja vikasietoisuus saadaan mahdollisemman korkeaksi. Palvelin- ja virustorjuntaohjelmat on pidettävä ajan tasalla. Jos mahdollista, kannattaa muutokset ja muut kokeilut tehdä testiympäristössä, ennen kuin ne tehdään tuotantoympäristössä.

Tutkintotyötä tehdessäni heräsi ajatus, että Exchange -sähköpostijärjestelmän katastrofisuunnitelma voisi olla hyvä lopputyön aihe seuraaville opiskelijoille. Yrityksillä, joilla on käytössä Active Directory -palvelut, on monesti käytössä myös Microsoftin Exhange -sähköpostipalvelu. Sähköpostipalvelut ovat todella kriittisessä asemassa nykyajan yrityksissä.

6 Sanasto

OSI X.500
Vuonna 1998 syntynyt avoin hakemistopalvelustandardi, jonka avulla sovellukset keskustelevat verkkoon hajautettujen palvelimien kanssa OSI -pinoa käyttäen.

LDAP
Lightweight Directory Access Protocol. LDAP on kevyt ja yksinkertainen yhteystapa OSI X.500 -hakemistopalveluun. LDAP kulkee TCP:n tai muun luotettavan protokollan päällä ja tarjoaa vain tärkeimmät X.500:n määrittelemistä palveluista.

TCP
Trasmission Control Protocol. TCP ohjaa datan lähetys- ja vastaanottoprosessia.

DNS
Domain Name System. Internetin nimipalvelujärjestelmä, joka kääntää Internetin verkkotunnukset (www.firma.fi) IP -osoitteiksi.

IP
Internet Proctocol. Verkkokerroksen protokolla, jonka tehtävänä on huolehtia IP -tietoliikennepakettien toimittamisesta perille IP-osoitteiden perusteella.

Replikointitopologia
Replikointitopologia muodostuu automaattisesti Active Directory -ympäristön rakentuessa. Näin ohjauspalvelimet osaavat replikoida tietojaan keskenään.

Intersite Topology Generator (ISTG)
Yksi toimipaikan ohjauspalvelin omaa tämän roolin, jonka avulla se tarkastaa toimipaikan sisäisen replikointitopologian sekä luo tarvittavan yhteyden sillanpääpalvelimiin, jotka mahdollistavat toimipaikkojen välisen replikoinnin.

Kerberos
Kerberos on verkkotunnistusprotokolla, joka mahdollistaa vahvan tunnistuksen työasema/palvelinsovellutuksille, käyttäen hyväksi salaiseen avaimeen perustuvaa salausta.

HAL
Hardware Abstraction Layer. Laitetoimittajan antama laitekerros käyttöjärjestelmään.

DN
Distinquished Name. LDAP-hakemistoissa käytettävä nimeämismenetelmä, joka yksilöi objektin hakemistopuussa.

SID
Security Identifier. Windows-toimialueen objektin suojaustunnus, joka koostuu kaikille yhteisestä alkuosasta ja yksilöllisesti RID-tunnisteesta.

Inkrementaalinen varmistus
Kopioidaan täyden varmuuskopion jälkeen ainoastaan muuttuneet tiedostot. Palauttaminen tarvitsee toimiakseen viimeisen täyden varmistuksen ja sen jälkeen tehdyt inkrementtaaliset varmistukset. Tästä johtuen se on hitaampi vaihtoehto kuin differentiaalinen varmistus.

Differentiaalinen varmistus
Sisältää kaikki muuttuneet tiedostot täyden varmistuksen jälkeen. On nopeampi palauttaa kuin inkrementtaalinen varmistus, mutta vie enemmän tilaa ja itse varmistaminen on hidasta.

Lähteet

Kivimäki, Jyrki 2004. Inside Active Directory verkonhallinta. Helsinki: IT Press Oy.

Kouti Sakari & Seitsonen, Mika 2002. Inside Active Directory. Helsinki: Addison-Wesley .

Active Directory Disaster Recovery White Paper Microsoft Corporation 2000.

[1@] CMS Consulting [online] [viitattu 10.6.2005]. http://www.cms.ca/solutions/activedd

[2@] Microsoft Active Directory roles. [online][viitattu 15.1.2005]. http://support.microsoft.com/kb/197132

[3@] Microsoft TechNET [online][viitattu 9.3.2005]. http://www.microsoft.com/technet/

[4@] Microsoft WINBACKUP [online][viitattu 9.3.2005]. http://www.ntbackup.info/BackupAssist/msgadmin4.php

[5@] VERITAS Software [online][viitattu 9.3.2005]. http://www.veritas.com)

[6@] Computer Associates [online][viitattu 9.3.2005]. http://www3.ca.com)

[7@] EMC Legato [online][viitattu 10.3.2005]. http://www.legato.com

[8@] Ultrium - LTO [online][viitattu 10.3.2005]. http://www.ultrium.com

[9@] DLT TAPE [online][viitattu 12.3.2005]. www.dltape.com

[10@] Search SMB [online][viitattu 12.3.2005]. http://searchsmb.techtarget.com

[11@] Jari Sarja - Tietoturva [online][viitattu 12.3.2005]. http://sarja.internetix.fi/fi/sisalto/materiaalit/tietoturva

[12@] Hewlett-Packard 2005 [online][viitattu13.3.2005]. http://www.hp.com

[13@] Song Networks 2005 [online][viitattu13.3.2005]. http://www.tdcsong.fi/index.php?path=laitetila

[14@] Microsoft [online][viitattu13.3.2005]. http://www.microsoft.com/finland/products/windows2000/server/intro_advanced.htm

[15@] MikroBitti [online][viitattu13.3.2005]. http://www.mikrobitti.fi/nettijatkot/2003/04/raid/

[16@] AC&NC [online][viitattu13.3.2005]. http://www.acnc.com/04_01_00.html

Liite

Tausta ja lähtökohdat

Tämän katastrofisuunnitelman lähtökohtana on, että Yritys X:n Active Directory -ympäristössä ei ole käytössä yhtään toimivaa ohjauspalvelinta, ja näin ollen palvelimet tarvitsee palauttaa nauhalta. Tällainen katastrofitilanne voi olla kyseessä, jos koneet ovat rikkoutuneet fyysisesti tai virushyökkäyksen johdosta ohjauspalvelimet eivät voi enää käynnistyä normaalisti. Tällaista katastrofitilannetta varten yritykselle tarvitaan toimiva toipumissuunnitelma, jonka avulla voidaan Active Directoryn tuottamat verkkopalvelut palauttaa mahdollisimman nopeasti toimintakuntoon.

Toipumissuunnitelmassa oletetaan, että katastrofi ei ole ulottunut varmistuspalvelimeen ja itse varmistusnauhat ovat ehjiä. Yritys X:n case-tapauksessa he käyttävät Legato NetWorker -palautusjärjestelmää. Jos varmistuspalvelin on vioittunut, pitää katsoa erillinen Legaton ohje varmistuspalvelimen uudelleen asentamisesta:
http://web1.legato.com/infodev/publications/NetWorker/disrec/7.2/disrec.pdf

Ohjauspalvelimista on hyvä pitää ajan tasalla olevaa taulukkoa sen tärkeimmistä asetuksista:

- Levyn konfiguraatio. Tarpeellinen tieto koskee levyjen ja osioiden asemia ja kokoja. Mikäli levyt ovat vioittuneet, voidaan tämän tiedon avulla konfiguroida levyt uudestaan. Levykonfiguraatioiden pitää olla kunnossa, ennen kuin palautusta voidaan alkaa tekemään.
- Tietokoneen nimi. Tämä tarvitaan, jotta ohjauspalvelimen nimi voidaan palauttaa eikä näin ollen tarvitse muuttaa työasemien konfiguraatiota.
- Toimialueen nimen pitää olla tiedossa, sillä vaikka nimi ei muutu, pitää sitä varten mahdollisesti luoda uusi tietokonetili.
- Paikallinen järjestelmänvalvojan salasana. Ilman tätä tunnusta koneelle ei voi kirjautua palautuksen jälkeen eikä toimialuetiliä voida luoda. Lisäksi kyseistä tunnusta tarvitaan järjestelmän tilan palauttamiseen (system state).
- Lista siitä, onko ohjauspalvelimessa toiminnassa muita palvelinpalveluita, esim. Exchange -sähköpostipalvelu.

Ensimmäisen ohjauspalvelimen asentaminen

Kun ensimmäistä ohjauspalvelinta aletaan palauttaa, pitää olla tiedossa palvelimen paikallinen järjestelmävalvojan salasana (administrator). Ilman kyseistä tunnusta palvelinta ei voida käynnistää palauttamisen kannalta tärkeään Restore Moodiin. Toinen tarvittava tunnus on Domain Admin -tasolla oleva tunnus, jolla on kaikki oikeudet toimialueeseen.

Kohdepalvelin on tässä tapauksessa uusi palvelin, mihin uuden ohjauspalvelimen palautus tehdään. Tässä tapauksessa varalaite on lähes samaa mallia rikkoutuneen ohjauspalvelimen kanssa. Palvelinmalleissa on eroja, joten on tärkeää, että kaikki tarvittavat laitteistoajureita sisältävät cd:t ovat tallessa.

- Kopioidaan kohdepalvelimessa käytetyn RAID -järjestelmän käyttöjärjestelmäkohtainen ajuri levykkeelle tai cd:lle. Tässä tapauksessa se on Windows 2000 Server.
- Asennetaan kohdepalvelin Windows 2000 Server käyttöjärjestelmällä, joka on sama kuin rikkoutuneessa ohjauspalvelimessa oli.
- Tarkistetaan olemassa olevasta dokumentaatiosta, millä tietoturvapäivitystasolla (Service Pack) ohjauspalvelin oli ennen vikaantumista. Lisäksi asennetaan tarvittavat ”Hot Fix” -pikapäivitykset. Tarkoituksena on, että kohdepalvelin on mahdollisimman samanlainen kuin alkuperäinen ohjauspalvelin oli ennen vikaantumistaan.
- Nimetään kohdepalvelin samannimiseksi kuin rikkoutunut ohjauspalvelin oli sekä asetetaan palvelimen verkkoasetukset oikeaksi.

HUOM! Jos palautus tehdään erillisessä verkossa, joka on irti normaalista tuotantoverkosta pitää, ottaa huomioon muutama ylimääräinen seikka. Näihin seikkoihin palataan kohdassa: Palautuksen tekeminen.

Kopioidaan seuraavat asiat talteen kohdepalvelimesta:
C:\Winnt\System32\hall.dll
c:\boot.ini
c:\Winnt\Repair\setup.log

Legato Networkerin asentaminen kohdepalvelimeen

Kun kohdepalvelimeen on saatu asennettua käyttöjärjestelmä sekä tarvittavat päivitykset ja ajuri, voidaan tämän jälkeen kohdepalvelimeen asentaa Legaton NetWorker Client -asiakasohjelma. NetWorker Client -ohjelma löytyy Legaton mukana tulleelta asennus-CD:ltä tai Internetistä osoitteesta: www.legato.com/support/websupport.

ASENNETAAN sama NetWorker Client –versio kohdepalvelimeen, kuin hajonneessa ohjauspalvelimessa oli!

- Kirjaudutaan kohdepalvelimeen järjestelmävalvojan tunnuksella Client -ohjelman asentamiseksi.
- Ajetaan Setup.exe -niminen tiedosto networkr-nimisestä hakemistosta. Tämän kohdan voi ohittaa, jos CD:n automaattinen käynnistystoiminto (Autorun) on käytössä.
- Tervetuloa Networker asennukseen -ikkunasta, painetaan Next -näppäintä asennuksen jatkamiseksi.
- Hyväksytään Legaton lisenssisopimus. Tämän jälkeen jatketaan asentamista painamalla Next -näppäintä.
- Syötetään Yritys X:ää koskevat tiedot ja painetaan Next -näppäintä.
- Valitaan, mikä Legato NetWorker ohjelma halutaan asentaa: Client vai Server. Oletuksena on Client. Tässä tapauksessa asennetaan Client -ohjelma.
- NetWorker -asennus tarjoaa oletusasennuspolkua, hyväksytään se tai muutetaan halutuksi.
- Riippuen Legaton Client -versiosta, voi asennus kysyä, halutaanko asentaa LEGATO Licence Manager -ohjelma. Ei asenneta!
- Syötetään NetWorker -varmistuspalvelimen nimi, jolle annetaan oikeus ottaa yhteys kyseiseen kohdepalvelimeen. Jos lista jätetään tyhjäksi, voivat kaikki NetWorker -palvelimet tehdä palautuksia. Tämä voi olla turvallisuutta vaarantava tekijä. Listaa voi päivittää uudestaan asennuksen jälkeenkin.
- Painetaan Install -näppäintä asennuksen aloittamiseksi. Asennuksen jälkeen viimeistellään asennus painamalla Finish -nappia.

Kun NetWorker Client on onnistuneesti asennettu kohdepalvelimeen, pitää testata, saako se yhteyden varmistuspalvelimeen.
Start → Programs → LEGATO NetWorker → NetWorker Administrator. Valitaan, Connect to Server, syötetään varmistuspalve-

limen nimi ja painetaan OK. Jos kohdepalvelin saa yhteyden varmistuspalvelimeen, voidaan itse palauttaminen aloittaa. Jos palvelin ei vastaa, tarkistetaan verkonasetuksien vianselvitys.

Palautuksen tekeminen

- Avataan NetWorker Client -työkalu ja painetaan Recover -nappia. Ohjelma aukaisee resurssienhallintaikkunan.
- Valitaan listasta palautettava ohjauspalvelin XXAD ja painetaan OK.
- Valitaan kohde, johon palautus tehdään. Oletuksena on Client -ohjelman omaava kone, joten valintaa ei tarvitse muuttaa.
- Valitaan resurssinäkymästä alla olevat tiedostot käyttämällä hyväksi Mark -nappia:

C-levy
System DB (quota, database, WMI)
System Files (system tiedostot %systemroot%)
System State (AD, COM, Rekisteri, SYSVOL)

Kaikkia C-levyn tiedostoja ei kannata palauttaa. Normaalin asennuksen %systemroot% viittaa hakemistoon c:\Winnt.

Jos kohdepalvelin oli konfiguroitu omaan verkkoon tai muuten irti tuotantoverkosta, niin **c:\winnt\system32\drivers\etc\host** tiedosto keskeyttää yllä olevan palautuksen, kun se ei löydä Legaton varmistuspalvelinta.

Tämän ongelman välttämiseksi varmistetaan, että host -tiedostoon on lisätty varmistuspalvelimen nimi ja IP-osoite.

C:\Program files\nsr aiheuttaa myös samaa ongelmaa, sillä siellä sijaitsee Legaton Client -ohjelman tiedostoja, joissa myös viitataan varmistuspalvelimeen.

Palauttaminen kestää muutamasta minuutista useisiin tunteihin, riippuen varmistetun datan määrästä, verkonkuormasta ja nauhamedian nopeudesta. NetWorker työkalu näyttää palautuksen väliaikatietoja. Tiedon avulla on helppo seurata, miten palautus etenee. Kun palautus on saatu valmiiksi, pitää alla olevat tiedostot kopioida alkuperäisille paikoilleen. Tiedot otettiin talteen ennen palautuksen aloittamista kohdepalvelimesta:

c:\Winnt\System32\hall.dll
c:\boot.ini
c:\Winnt\Repair\setup.log

Kohdepalvelin on valmis ensimmäiseen uudelleenkäynnistykseen.

Ensimmäinen uudelleenkäynnistys

Palautettu ohjauspalvelin käynnistetään nyt uudelleen ensimmäisen kerran. Jos käynnistysvaiheessa tulee ilmoitus: inaccessible_boot_device, toimitaan edellisen kappaleen mukaan.

Jos kohdepalvelin käynnistyy kuitenkin normaalisti, pitää kirjautumisen jälkeen siivota laiteajureita manuaalisesti, sillä koneessa on tiedot vanhasta rikkoutuneesta ohjauspalvelimesta, ja siksi laiteajurit eivät toimi (Verkkokortti, Näytönohjain, RAID).

- Käytetään Device Manager Advance -työkalua ja poistetaan kyseistä työkalua käyttäen ongelmia aiheuttavat vanhat laiteajurit (Raid…).
- Ajetaan kohdepalvelimen uusien laitteiden/ohjelmien asennusvelho ja asennetaan tarvittavat laitteistoajurit ja protokollat.
- Toimialueen palautetun ohjauspalvelimen TCP/IP -protokolla voi aiheuttaa ongelmaa. Protokolla pitää poistaa ja asentaa eri tavalla kuin normaalisti. Tähän operaatioon löytyy tarkat ohjeet Microsoftin Support -sivuilta osoitteesta: http://support.microsoft.com/default.aspx?scid=kb;EN-US;q299451
- Lopuksi tyhjennetään koneen logitiedostot, jotta voidaan seurata helpommin mahdollisia uusia ongelmia.

Ongelmatilanteesta johtuva toinen uudelleenkäynnistys

Toinen uudelleenkäynnistys tehdään mahdollisen virheilmoituksen (inaccessible_boot_device) johdosta.

- Ei yritetä uudelleen käynnistää ohjauspalvelinta normaalisti, vaan käynnistetään ohjauspalvelinasennus CD:ltä Restore Moodiin. Vika ilmeisesti johtuu siitä, ettei ohjauspalvelin tunnista uuden ohjauspalvelimen RAID-järjestelmää.
- Kopioidaan oikeat RAID-ajurit korpulta, jotta järjestelmä -levyt tulevat näkyviin. Restore Moodin Manual Repair -toiminnon avulla Windows -käyttöjärjestelmä korjaa muutkin mahdolliset laitteistovirheet.
- Kun kohdepalvelin käynnistyy ilman virheilmoituksia, aloitetaan manuaalinen laiteajureiden putsaaminen, jota käsittelimme aikaisemmin.

Ohjauspalvelin on nyt valmis Active Directoryn palauttamiseen.

Active Directoryn palauttaminen

Kun uusi ohjauspalvelin on saatu palautettua sellaiseen kuntoon, että laitteet toimivat moitteetta, on vuorossa Active Directoryn tietokannan asentaminen authoratiiviseen moodiin (Authorative). Palautettu ohjauspalvelin uudelleenkäynnistetään Directory Services Restore Moodiin. Tässä tilassa ohjauspalvelimelle tehdään Active Directory –toimenpide, jossa se asetetaan Authorative –moodiin.

Tässä palautuksessa käytetään Authoratiivista palautusta, sillä ympäristössä ei ole muita ohjauspalvelimia, jotka voisivat replikoida tiedot. Lisätietoja asiasta löytyy osoitteesta:
http://support.microsoft.com/default.aspx?scid=kb;en-us;241594&sd=tech

Käytetään komentoriviltä ntdsutil-työkalua.
c:\>ntdsutil
>authoratitave restore
>restore database
>ok

Kun tämä vaihe on tehty, ohjauspalvelin uudelleen käynnistetään normaalisti. Kirjautumisen jälkeen voidaan aloittaa SYSVOL:in uudelleenrakennus.

Acitve Directory -tietokannan palauttaminen

Authoratiivisen palautuksen jälkeen rakennetaan SYSVOL -hakemisto uudestaan. SYSVOL on toimialueen Active Directory -palvelimessa tai palvelimissa paikallisesti sijaitseva tietty hakemisto- ja tietokokonaisuus, joita FRS-palvelu replikoi muille Active Directory -ohjauspalvelimille. Työasemat ottavat yhteyksiä SYSVOL -hakemistorakenteen alla oleviin muihin resursseihin käyttämällä jaettuja NETLOGON- ja SYSVOL -hakemistoja.

Oletuspolku SYSVOL-rakenteelle on %systemdrive%\WINNT-hakemisto. Hakemisto voi olla asennettuna mille tahansa NTFS-partitiolle.

Konfikuroidaan SYSVOL-replikointi authoratiiviseen moodiin rekisteriavaimen Burflags -avulla, jotta palvelin replikoi muille ohjauspalvelimille oikeat tiedot.

- Start → Run →Regedit
- Rekisteriavain löytyy haarasta: HKEY_Local_Machine\System\CurrentControlSet\Services\NtFrs\Parameters\BackUp/Restore\Pocess at Startup
- Tuplaklikataan BurFlags.
- Edit DWORD Value, kirjoitetaan D4 ja painetaan ENTER
- Poistutaan Regedit:stä.
- Tämän jälkeen kopioidaan c:\winnt\sysvol\domain\ntfrs_PreExisting_See_Eventlog hakemistosta Policies ja Scripts hakemistot c:\winnt\sysvol\domain hakemistoon.
- Uudelleen käynnistetään ohjauspalvelin ja tarkistetaan, näkyykö NETLOGON share. Komentoriviltä Net Share komento.

Lisätietoja: http://support.microsoft.com/default.aspx?scid=kb;en-us;315457

Active Directoryn toiminnan testaus

Kun Active Directory on saatu palautettua edellisten hienosäätöjen jälkeen, tulee toimivuus testata huolellisesti. Palautus aiheuttaa viiveen (1-60 min), jonka jälkeen Active Directoryn SYSVOL ja aktiiviset jaot tulevat toimintaan ja replikointi alkaa toimia (tässä vaiheessa ei vielä replikointi -kumppaneita). Vasta tämän jälkeen Active Directory palvelut toimivat normaalisti. Alla on listattuna asioita, jotka kannattaa testata toiminnan varmistamiseksi:

- Näkyvätkö kaikki organisaation objektit (hakemisto, yksiköt, käyttäjät)?
- Testataan replikointi mahdolliselle toiselle Active Directory -ohjauspalvelimelle
- Pääsevätkö käyttäjät kirjautumaan toimialueelle.
- Käyttäjäobjektin muokkaus onnistuu
- Käyttäjäobjektin poisto ja lisäys onnistuu
- Toimivatko oikeellisuustasot
- Toimiiko salasanaresetointi käyttäjän tilissä.
- Testataan Group Policy -ryhmäkäytännöt ja niiden toimivuus.
- Testataan verkkojaot.
- Tarkistetaan logitiedot.