

**Exchange 2003-2007 migraatio Quang Tri Teachers' Training  
College Dong Ha Vietnam**

Mika Aro

Opinnäytetyö  
Tietojenkäsittely  
2013



<b>Mika Aro</b>	<b>Ryhmä tai aloitusvuosi</b> TIKO2004
<b>Opinnäytetyön nimi</b> Exchange 2003-2007 Migraatio Quang Tri Teachers Training College Dong Ha Vietnam	<b>Sivu- ja liitesivumäärä</b> 56
Olavi Korhonen.	
<p>Opinnäytetyön tarkoituksena oli selvittää kuinka migraatio tehdään Exchange 2003 ympäristöstä Exchange 2007 ympäristöön. Kyseessä on fiktiivinen työ eli koulu on olemassa ja opinnäytetyössä mainitut ongelmat sekä lähtökohdat ovat oikeat. Työ on fiktiivinen siksi, että työlle ei ole varsinaisesti tilaajaa eikä kyseistä ympäristöä tulla oikeasti pystyttämään. Tavoitteena oli tehdä oikea migraatio kaikkine vaiheineen. Tuloksista ilmenee se että migraatio näillä ohjeilla onnistuu..</p> <p>Tämän opinnäytetyön avulla saadaan migraatiosta tarkka käsitys. ja voi toimia oppaana migraatioapua etsiville</p>	
Exchange 2003, Exchange 2007 , Vietnam, Dong Ha	

Business information Technology

<p><b>Author</b> Mika Aro</p>	<p><b>Group or year of entry</b> Tiko2004</p>
<p><b>The title of thesis</b> The migration from Exchange 2003 to Exchange 2007 at Quang Tri Teachers' Training College in Dong Ha, Vietnam</p>	<p><b>Number of pages and appendices</b> 56</p>
<p><b>Supervisor</b> Olavi Korhonen</p>	
<p>The purpose of this thesis was to clarify how the migration from the Exchange 2003 environment to the Exchange 2007 environment is done.</p> <p>The study was set to take place at Quang Tri Teachers' Training College in Dong Ha, Vietnam. The institution in questions does exist but it was used as a fictitious environment as it is unlikely that such a migration would happen there. However, the migration related concepts and problems and various phases were real and relevant as they would be in a real environment.</p> <p>The result of this thesis was a guidebook on how to carry out a migration between the Exchange 2003 and 2007 environments. The thesis indicated that the migration can successfully be done according to the guidelines and instructions in the guidebook.</p> <p>The thesis concludes that the guidelines regarding the migration can be beneficial to those with interest in Exchange 2003-2007 migration and this study provides the reader with detailed information and understanding on how the migration should be done.</p>	
<p><b>Key words</b> Exchange 2003, 2007, Migration Vietnam, Dong Ha</p>	

1.	Lyhenteet .....	1
2.	Johdanto ja tavoitteet.....	2
3.	Ongelman kuvaus.....	4
4.	Exchange Server 2003 ja 2007 väliset erot .....	5
4.1	Exchange Server 2003.....	5
4.2	Exchange Server 2007.....	8
5.	Exchange 2007 – migraatioprojektin dokumenttien lukijalle .....	10
6.	Suosittelava Exchange 2007 -ympäristö .....	10
6.1	Siivotaan Exchange 2003 –ympäristö .....	11
7.	Arkkitehtuurisuunnitelman lähtötiedot .....	11
7.1	Microsoft Active Director Topologi Diagrammer .....	12
7.2	Sähköpostilaatikoiden määrä .....	12
7.3	Postilaatikoiden kokorajoitus .....	12
7.4	Sähköpostipalveluiden sijoituspaikka.....	12
7.5	Sähköpostiliikenteen reititykset .....	13
7.6	Työasemat.....	13
8.	Exchange 2007 -arkkitehtuurin palvelimet .....	14
8.1	Edge Transport Server.....	15
8.2	HUB transport Server .....	15
8.3	Client Access Server .....	15
8.4	Mailbox Server .....	16
8.5	Skaalautuvuus .....	16
8.6	Tietoturva.....	16
9.	Exchange 2007 –infrastruktuurin lokit.....	18
10.	Exchange 2007 –ympäristön asentaminen.....	19
10.1	WINS-palveluiden tarve.....	19
10.2	PKI-diagnostiikka .....	20
10.3	Exchange 2007 –sähköpostipalvelinten levyjen valmisteleminen –diskpart.....	20
10.4	Edellytykset Exchange 2007:n asentamiseksi.....	21
10.5	Palvelininfrastruktuurin valmisteleminen.....	23
10.6	Tietoliikenteen reititykset -default gateway .....	23
10.7	CAS-palvelinten asentaminen.....	24
10.8	Hub-palvelimen asentaminen.....	25
10.8.1	Sähköpostin ”ulkoiset” reititykset Hub-palvelimella .....	25
10.9	Sähköpostin ”sisäiset reititykset koulujen välillä.....	27
10.10	NDR -kuittausten käsitteleminen .....	28
10.11	Edge -palvelinten asentaminen.....	28
10.12	Edge-palvelinten konfiguroiminen .....	30
10.13	CCR -mailbox palvelinten asentaminen .....	31
10.14	Asennetaan käyttöjärjestelmän perus-klusterointi.....	32
10.15	Asennetaan CCR-klusterin aktiivinen ”node”.....	33
10.16	Asennetaan CCR-Klusterin passiivinen ”node”.....	34

10.17 Sähköpostiklusterin palvelut -käynnistysjärjestys .....	35
10.18 Konfiguroidaan Client Access –palvelin tehtäviinsä .....	35
10.19 Rakennetaan Network Load Balancing CAS-palvelimelle .....	36
10.20 Client Access –palvelinten varmenteiden käsitteleminen .....	37
10.21 Tarkistetaan Exchange-palvelinten konfiguraatiot .....	38
10.22 Outlook Web Access –kutsu helpoksi .....	38
10.23 Exchange palvelinten paikalliset administrator ylläpitoryhmät .....	39
10.24 CCR -klusterin toiminnallisuuden testaaminen .....	40
10.27 DTC konfiguraation avaaminen .....	41
10.28 SPAM filteröinti Sender-ID .....	42
10.29 SPAM filteröinti SPF .....	42
10.30 SPAM –filterointi: SIDF ja DKIM .....	43
11. Exchange 2003->Exchange 2007 migraation vaiheet .....	44
11.1 Migraation kulku .....	44
11.2 Sähköpostilaatikoiden migrointi .....	45
11.3 Alustavat toimenpiteet .....	45
11.4 Sähköpostilaatikoiden ym. siirtäminen .....	46
11.5 Vanhan järjestelmän alasajo .....	46
11.6 Käsien tehdyt SMTP osoitteet .....	47
11.7 Migraatiotunnukset .....	47
11.8 Palvelinten määrä .....	47
12. Outlook 2003 profilit .....	50
13. Tietoliikenteen määrät .....	51
14. Sähköpostijärjestelmän mahdollisesti kokemat nykyiset/tulevat haasteet .....	52
15. Pohdinta .....	53
16. Lähteet .....	54
Liitteet .....	56

## 1. Lyhenteet

AD	Active Directory. Käyttäjätietokanta ja hakemisto palvelu.
CAS	Client Acces server. Palvelinrooli.
CRC	Cycling redundance check. Käsite, jolla tarkasteavaimen avulla pyritään havaitsemaan virheitä, joita on voinut tapahtua tiedonsiirron tai säilytyksen aikana.
DNS	Domain Naming Service. Sen perustoimintoihin kuuluu muuttaa verkkonimet ip osoitteiksi ja toisinpäin.
EDB	Exchange Databace Exchange tallentaa datan EDB tiedostoihin
HTTP	Hyper Transfer Protocol. Hypertekstin siirtoprotokolla, jota käytetään tiedonsiirroissa selaimissa ja palvelimissa
IIS	Internet Information Services. Microsoftin palvelinohjelmisto kokonaisuus
IMAP	Internet Message Access Protocol. Sähköpostien lukemiseen tarkoitettu protokolla.
IP	Internet Orotocol. Protokolla joka huolehtii IP-tietoliikennepakettien toimittamisesta perille. On olemassa kaksi erilaista versiota IPv4 ja IPv6.
MBX	Mailbox. Palvelinrooli.
MIGRAATIO	Tietotekniikassa migraatio tarkoittaa tietokoneessa suorituksessa olevan tehtävän siirtoa kesken suorituksen toiseen tietokoneeseen (tai saman tietokoneen toiseen suorittimeen), mutta myös tietojen siirtämistä ohjelman eri versioiden välillä, esim. otettaessa käyttöön ohjelman uudempi versio.
OWA	Outlook Wep App. Selainpohjainen sähköpostiohjelma.
POP	Post Office Protocol. Sähköpostien hakemiseen tarkoitettu protokolla.
RAM	Random Access Memory. Keskusmuisti, jota tietokoneet käyttävät työmuistina.
RSG	Recovery Storage Group. Sähköpostilaatikoiden ylläpitotyökalu, jolla voidaan palauttaa esim. sähköpostilaatikoita.
SMTP	Simple Mail Transfer Protocol. Käytetään viestien välittämiseen sähköpostipalvelimien kesken.
SSL	Secure Socket Layer. Tietoverkkosalausprotokolla.

## 2. Johdanto ja tavoitteet

Opinnäytetyössä tutustutaan Microsoft Exchange 2003 ja Exchange 2007 väliseen migraatioon. Opinnäytetyöni on teoreettinen työ, jonka taustalla on kuvitteellinen toimeksianto Dong Ha kaupungissa Vietnamissa sijaitsevaan kouluun. Kyseinen migraatio on suoritettu testilaboratoriossa Suomessa oikeilla palvelimilla.

Kaikki asennusvaiheet on tehty siinä järjestyksessä kuin ne tässä opinnäytetyössä kuvataan.

Tarkoituksena oli pystyttää toimiva Exchange 2007 jatkuvan replikoinnin klusteri.

Näiden ohjeiden perusteella pitäisi olla mahdollista suorittaa migraatio Exchange 2003 ja Exchange 2007 välillä.

Tavoitteena on myös, että opinnäytetyötä lukeva henkilö ymmärtäisi ohjelmiston ja ympäristön suunnittelun, asennuksen ja hallinnointityökalut siten, että migraatio voidaan niiden perusteella suorittaa.

Uusi Exchange 2007:n mahdollistama CCR (Cluster Continuous Replication) –klusterointi poistaa postilaatikkopalvelimilta yhden heikon lenkin muodostaman riskin. Klusterin kumpikin palvelin käyttää omia fyysisiä levyjään palvelimet voidaan sijoittaa fyysisesti eri tiloihin.

Palveluiden siirto vikaantuneelta palvelimelta toimivalle palvelimelle ja aikanaan sieltä takaisin on täysin automaattista, joskin toki myös ylläpitäjän määriteltävissä.

Exchange itsessään käyttää tässä klusterointimallissa asynkronista transaktiologioiden replikointia palvelimelta toiselle, mahdollistaen näin myös varmuuskopioiden ottamisen passiiviselta palvelimelta. Tämä tarjoaa huomattavasti laajemman aikaikkunan varmuuskopiointiin.

SMTP- ja client –toiminnot on kahdennettu käyttäen Exchange 2007:n HUB/CAS –palvelinten välillä vikasietoista NLB –kuormanjakoa (Network Load Balancing).

Uusi Exchange 2007 vaatii toimiakseen vähintään 2003-tasoisesta AD -ympäristön. On kuitenkin suotavaa, että myös uusi AD on 2008 tasoa parhaan toimivuuden takaamiseksi

Palveluiden siirto nykyisistä järjestelmistä uuteen järjestelmään tapahtuu erillisellä transiitio projektilla, joka sisältää seuraavat vaiheet.

- palvelinympäristön tarkempi suunnittelu ja asentaminen
- Exchange roolien suunnittelu ja asentaminen
- Palveluun liittyvien ulkopuolisten rajapintojen suunnittelu ja muutosten vaiheistaminen siten, että käyttökätköt ovat vähäisiä.

- Käyttäjien migrointi nykyisistä järjestelmistä uuteen järjestelmään
- Vanhan sähköpostipalvelimen alasajo
- AD ympäristön perustaminen

Rajaus:

Tämä lopputyö keskittyy ainoastaan migraatioon Dong Ha:n ympäristön osalta. Lopputyö tulee olemaan ympäristökuvaus koulun vanhasta järjestelmästä (ei siis sisällä AD kuvausta eikä verkko/laitekuvausta sen tarkemmin). Migraatio lähtee siitä oletuksesta, että vanha AD on tarkastettu ja kunnossa. Uusi AD on pystytetty ja alustavat toimenpiteet on tehty esim. vanhan AD:n tieto on migroitu uuteen 2008 AD:iin

Tämä lopputyö ei ota kantaa AD konfiguraatioihin. Se miten AD liittyy tähän migraatioon on seuraava.

Exchange sähköpostijärjestelmä on vahvasti osa AD:ta mutta pitää ottaa huomioon, että AD toimii ilman Exchange järjestelmää mutta Exchange ei voi toimia ilman AD:ta.



### 3. Ongelman kuvaus

Tämän opinnäytetyön historia ulottuu vuosiin 1998/1999. Kyseisinä vuosina kävin ensimmäiset kertani Vietnamsissa.

Varsinaisen idean opinnäytetyöhön sain vieraillessani Dong Ha:n kouluissa. Rakennukset sijaitsivat noin viiden kilometrin etäisyydellä toisistaan. Huomioitavaa kyseisten koulujen tietoteknisissä laitteissa oli se, että laitteet oli saatu erinäisistä paikoista lahjoituksena. Kaikki koneet olivat työryhmäverkossa. Verkkokaapelointi oli toteutettu ohut ethernet tekniikalla. Palvelimen käyttöjärjestelmänä oli Novell Netware 3.1.. Työasemiin oli myös asennettu Novell, lahjoituksena Australiasta. Hyvin pian kävi kuitenkin ilmi, että luokkaa ei ollut käytetty kahteen vuoteen johtuen järjestelmän vikaantumisesta. Koulun henkilökunta ei enää ollut kyennyt korjaamaan ongelmaa.

Kouluilta löytyi myös Windows 95 työasemia varustettuna Windows NT 3.5.1 työasema palvelimella. Kaapelointi myös näissä luokissa oli varustettu ohut Ethernet kaapeloinnilla. Lähtökohdat olivat aluksi varsin mielenkiintoiset. Myöhemmin koululle hankittiin työasemien uusimisen yhteydessä Exchange 2003 ja Windows Server 2003.

Varsinaista verkkoa ei koulujen välillä ole ollut koskaan. Myöskään opettajilla ei ole ollut varsinaisesti toimivaa sähköpostijärjestelmää olemassa ennen vuotta 2003. Aluksi opettajien sähköpostit olivat yhteislaatikoita operaattorin palvelimella. Vuonna 2003 toteutetun muutoksen jälkeen yhteispostilaatikat siirtyivät koulun postipalvelimelle ja henkilökohtaiset postilaatikat otettiin käyttöön.

Tämän opinnäytetyön tarkoitus on tehdä kattava migraatio, jossa palvelimet uusitaan Windows 2008 ja Exchange 2007 ohjelmiin. Migraatiossa uusitaan Quang Tri Teachers Training College (QTTTC) ympäristö.

Kyseessä on ns. teoreettinen työ. Tämän opinnäytetyön tekeminen on suoritettu olettaen että oikea toimeksi anto olisi saatu ja projektin aloitus olisi hyväksytty. Lopputyötä tehtäessä kaikki vaiheet on otettu huomioon ja laitteisto on asennettu ja vaiheet on testattu.

## 4. Exchange Server 2003 ja 2007 väliset erot

### 4.1 Exchange Server 2003

Exchange 2003 Server on monimutkainen sähköpostijärjestelmä joka on riippuvainen Microsoft Active Directory:sta. Useat ydin komponentit työskentelevät yhteistyössä näin muodostaen toimivan ja tehokkaan sähköpostijärjestelmän.

Alla olevat kuvat osoittavat Exchange 2003 Server ydin palvelut. Palveluita on kuitenkin enemmän kuin kuvasta näkyy. Exchange 2003 Serveriin liittyviä palveluita ovat esim .

WWW julkaisu palvelu (WWW Publishing Service)

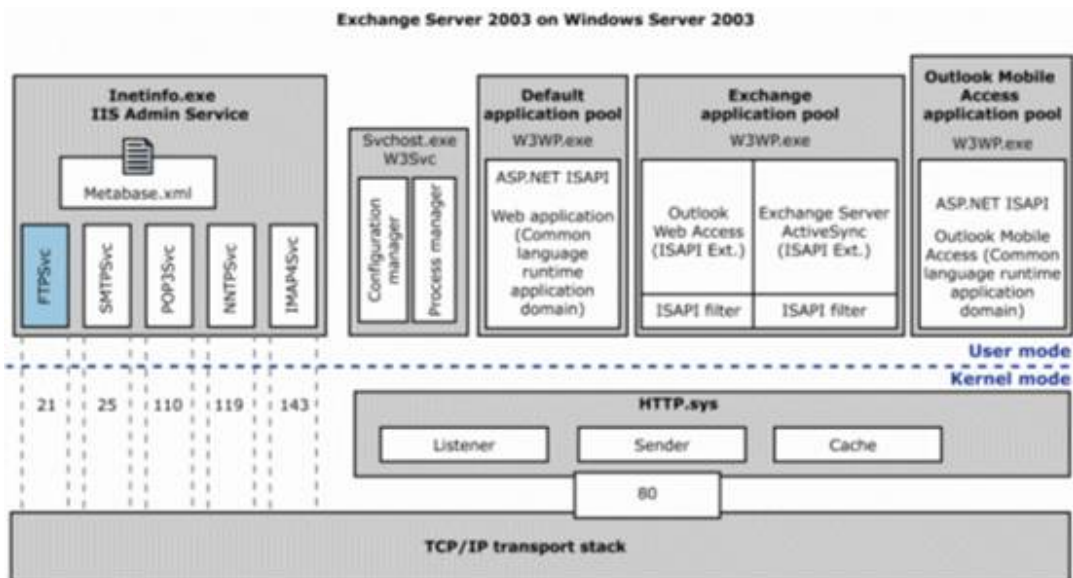
SMTP viestien välitys protokolla (Simple Transfer Protocol)

IIS Microsoftin palvelinohjaus kokonaisuus (Internet Information Service)

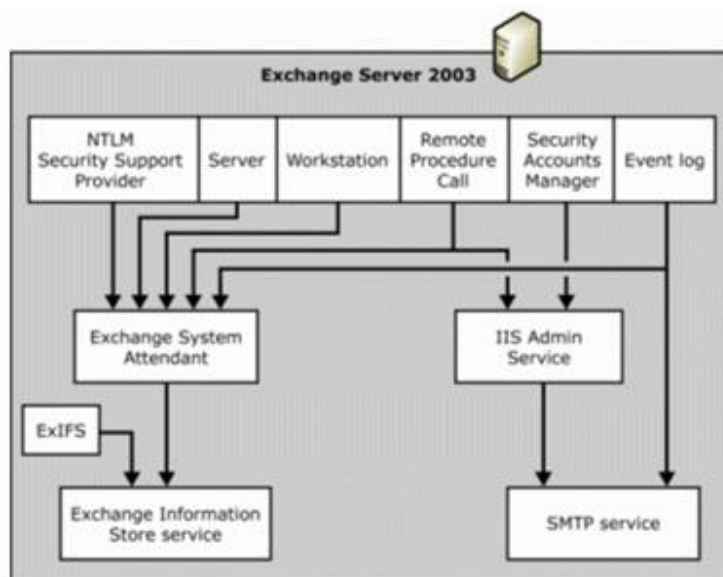
Exchange 2003 Server mahdollisti myös laajojen järjestelmien rakentamisen. Exchange 2003 Server oli myös vikasietoisempi kuin edeltäjänsä Exchange 2000 Server. Tällä Exchange 2003 Server osiolla yritän kuvata kuvilla miten järjestelmä toimii. Kuvat esittävät mitä toimintoja taustalla pyörii, vaikka loppukäyttäjälle näkyy ainoastaan postilaatikko ja kalenteri. Luvun 4.1 kuvia voi verrata luvun 4.2 kuviin. Seuraava luku esittelee Exchange 2007 Serverin yleisellä tasolla.

Microsoft Exchange Event	Monitors folders and fires events, for Exchange 5.5-compatible server ...	Manual
Microsoft Exchange IMAP4	Provides Internet Message Access Protocol (IMAP4) Services to clients. ...	Disabled
Microsoft Exchange Information Store	Manages the Microsoft Exchange Information Store. This includes mailb...	Started Automatic
Microsoft Exchange Management	Provides Exchange management information using Windows Managem...	Started Automatic
Microsoft Exchange MTA Stacks	Provides Microsoft Exchange X.400 services. Exchange X.400 services ...	Started Automatic
Microsoft Exchange POP3	Provides Post Office Protocol version 3 (POP3) Services to clients. If thi...	Disabled
Microsoft Exchange Quota Service		Manual
Microsoft Exchange Routing Engine	Provides topology and routing information to Exchange Server 2003 ser...	Started Automatic
Microsoft Exchange Site Replication Service		Disabled
Microsoft Exchange System Attendant	Provides monitoring, maintenance, and Active Directory lookup services...	Started Automatic
Microsoft Identity Integration Server	Enables integration and management of identity information across mult...	Manual
Microsoft iSCSI Initiator Service	Manages Internet SCSI (iSCSI) sessions from this computer to remote IS...	Manual
Microsoft Search	Creates full-text indexes on content and properties of structured and s...	Started Automatic

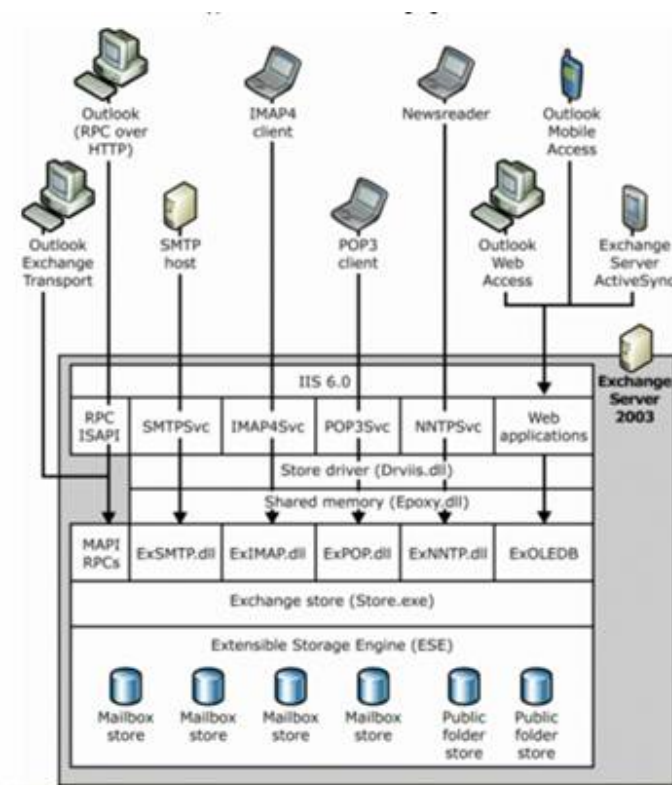
Kuva 1. Exchange ydinpalvelut <http://www.msexchange.org/articles-tutorials/exchange-server-2003/planning-architecture/Exchange-Internals-How-Exchange-Core-Components-work-together.html> by Marc Grote [Published on 15 June 2006 / Last Updated on 15 June 2006]



Kuva 2. Web palvelut Microsoft Exchange 2003 (Lähde: Microsoft: <http://www.msexchange.org/articles-tutorials/exchange-server-2003/planning-architecture/Exchange-Internals-How-Exchange-Core-Components-work-together.html> by Marc Grote [Published on 15 June 2006 / Last Updated on 15 June 2006])



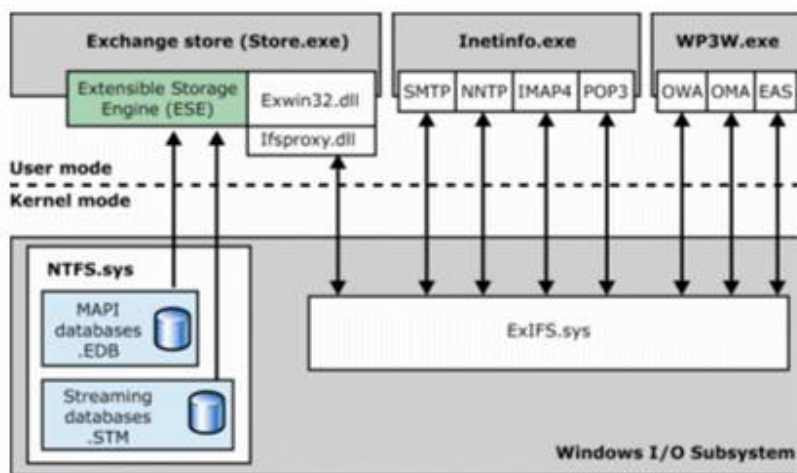
Kuva 3. Exchange ja Windows palveluiden riippuvuudet (Lähde Microsoft: <http://www.msexchange.org/articles-tutorials/exchange-server-2003/planning-architecture/Exchange-Internals-How-Exchange-Core-Components-work-together.html> by Marc Grote [Published on 15 June 2006 / Last Updated on 15 June 2006])



Kuva 4. Exchange palvelut työskentelevät yhdessä (Lähde: Microsoft:

<http://www.msexchange.org/articles-tutorials/exchange-server-2003/planning-architecture/Exchange-Internals-How-Exchange-Core-Components-work-together.html>

by Marc Grote [Published on 15 June 2006 / Last Updated on 15 June 2006])



Kuva 5. EXiFS Exchange 2003 palvelimessa (lähde: Microsoft:

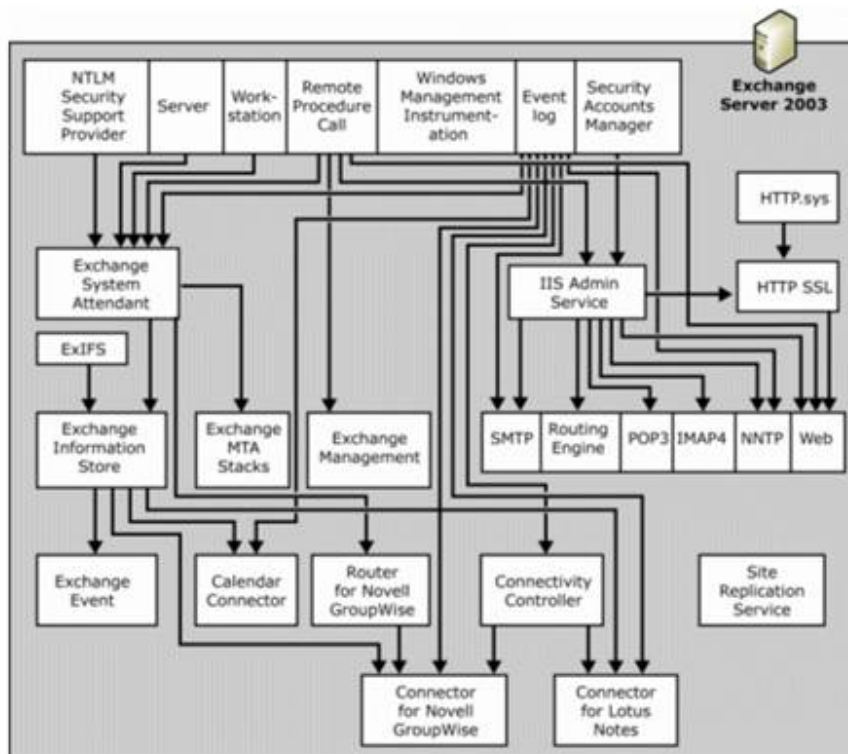
<http://www.msexchange.org/articles-tutorials/exchange-server-2003/planning-architecture/Exchange-Internals-How-Exchange-Core-Components-work-together.html>

by Marc Grote [Published on 15 June 2006 / Last Updated on 15 June 2006] )

## 4.2 Exchange Server 2007

Uusi Exchange 2007 Server on paljon enemmän kuin pelkkä sähköpostijärjestelmä.

Se on paljon muutakin kuin sähköposti. se on kalenteri, reaaliaikainen keskustelu ohjelma kuten esim. Microsoft messenger. kaikkien näiden osien tulee toimia yhdessä. Exchange on myös entistä enemmän riippuvainen DNS, Active Directory ja IIS palveluista. Alla olevat kuvat kertovat, mitkä palvelut ovat uusia verrattuna Exchange 2003 palvelimeen ja mitkä palvelut ovat vain ja ainoastaan Exchange 2003 palvelimessa.

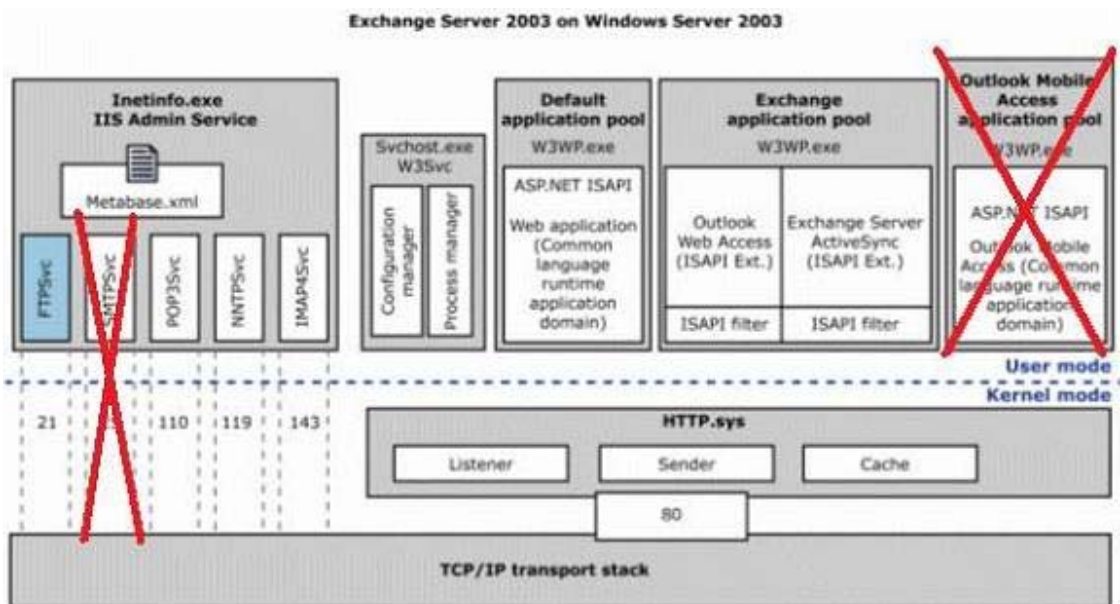


Kuva 6. Kaikki Exchange ja Windows palvelut ”käsi kädessä” (Lähde Microsoft: <http://www.msexchange.org/articles-tutorials/exchange-server-2003/planning-architecture/Exchange-Internals-How-Exchange-Core-Components-work-together.html>)

by Marc Grote [Published on 24 July 2007 / Last Updated on 24 July 2007] )

Microsoft Exchange Active Directory Topology Service	Provides Active Directory topology information to Exchange services. If t...
Microsoft Exchange Anti-spam Update	The Microsoft Forefront Security for Exchange Server anti-spam update ...
Microsoft Exchange EdgeSync	The Microsoft Exchange EdgeSync Service.
Microsoft Exchange File Distribution	Microsoft Exchange File Distribution Service.
Microsoft Exchange IMAP4	Provides Internet Message Access Protocol (IMAP4) Services to clients. I...
Microsoft Exchange Information Store	Manages the Microsoft Exchange Information Store. This includes mailbo...
Microsoft Exchange Mail Submission	Submits messages from the Mailbox server to the Hub Transport servers.
Microsoft Exchange Mailbox Assistants	Performs background processing of mailboxes in the Exchange store.
Microsoft Exchange Monitoring	Allows applications to call the Exchange diagnostic cmdlets.
Microsoft Exchange POP3	Provides Post Office Protocol version 3 (POP3) Services to clients. If this ...
Microsoft Exchange Replication Service	The Microsoft Exchange Replication Service provides replication functiona...
Microsoft Exchange Search Indexer	Drives indexing of mailbox content, which improves the performance of c...
Microsoft Exchange Service Host	Provides a host for several Microsoft Exchange services
Microsoft Exchange Speech Engine	Microsoft Exchange Speech Engine
Microsoft Exchange System Attendant	Provides monitoring, maintenance, and Active Directory lookup services, ...
Microsoft Exchange Transport	The Microsoft Exchange Transport Service.
Microsoft Exchange Transport Log Search	Provides remote search capability for Microsoft Exchange Transport log fi...
Microsoft Search (Exchange)	Quickly creates full-text indexes on content and properties of structured ...

Kuva 7. Exchange 2007 ydinpalvelut (Lähde: Microsoft: <http://www.msexchange.org/articles-tutorials/exchange-server-2007/planning-architecture/how-exchange-server-2007-core-services-work-together.html> by Marc Grote [Published on 24 July 2007 / Last Updated on 24 July 2007])



Kuva 8. Exchange palveluiden integrointi (lähde: Microsoft: <http://www.msexchange.org/articles-tutorials/exchange-server-2007/planning-architecture/how-exchange-server-2007-core-services-work-together.html> by Marc Grote [Published on 24 July 2007 / Last Updated on 24 July 2007])

## **5. Exchange 2007 – migraatioprojektin dokumenttien lukijalle**

Tämä dokumentti on Exchange 2007 -migraatioprojektin arkkitehtuurisuunnitelman päädokumentti. Dokumentti antaa yleiskuvan määrittely- ja suunnitteluvaiheen toteutuksesta. Dokumentin kohderyhmänä ovat kaikki Exchange 2007 -migraatioprojektin sidosryhmät.

Tavoitteena ei ole ollut tehdä kaiken kattavaa “oppikirjaa”, vaan Quang Tri Teachers Training Collegen arkkitehtuurisuunnitelma. Tarkentavaa tietoa on saatavilla yllin kyllin sen jälkeen kun perusratkaisut on tehty tässä suunnitelmassa.

## **6. Suositeltava Exchange 2007 -ympäristö**

Suunniteltu Exchange 2007 -ympäristö perustuu Teachers Training Collegen metsän käyttämiseen. Alustava arvio koulun Exchange konfiguraation palvelinmäärälle on 4 kappaletta.

Exchange 2007 SP1 ei suostu asentumaan Windows 2008 read-only domain controller-palvelimeen. Tämä on hyvä tietää kun arvioidaan muualla kuin Dong Ha:ssa sijaitsevien toimipisteiden konfiguraatioita.

## 6.1 Siivotaan Exchange 2003 –ympäristö

Ennen migraatiota on hyvää aikaa siivota nykyistä ympäristöä. Esimerkiksi sähköpostilaatikoiden attribuutit ym. kannattaa korjata kohdalleen.

Tavoitteena on, että migraation aikana ei tarvitse tehdä käsityötä sähköpostijärjestelmän korjaamiseksi eikä myöskään tehdä kehitystyötä ja muuttaa migraatioprosessia.

## 7. Arkkitehtuurisuunnitelman lähtötiedot

Määrittely- ja suunnitteluprojektin oleellisiin taustatietoihin kuuluvat kuvaukset ja kerätyt omakohtaiset tiedot koulun tietotekniikka ympäristöstä. Tiedot on kerätty Vietvoc projektin dokumenteista ja haastattelemalle Vietvoc projektin asiantuntijoita.

Tietoja on kerätty mm. seuraavista asioista:

- toimipisteiden määrät
- työasemien määrät toimipisteissä
- verkkojen tietoliikennenopeudet
- nykyinen dns infrastruktuuri
- hallinnan keskittäminen ja hajauttaminen
- IT ympäristössä vaikuttavat palveluntarjoajat
- odotettavissa olevat muutokset
- tietoturvan pysyväismääräykset
- sähköpostijärjestelmän rakenne
- kaikki seikat, joiden takia järjestelmän osia olisi eristettävä toisistaan
- Teachers Training Collegen toimialueiden hallintakoneiden määrät ja sijoittelut toimipisteisiin
- kriittisten palvelinten valvonnan tilanne
- nykyiset käyttöjärjestelmäversiot, korjauspaketit jne.



- järjestelmänhallinnan rakenne

### **7.1 Microsoft Active Director Topologi Diagrammer**

Tehokas väline Active Director- ympäristöjen toimipisterakenteiden kartoittamiseen on Microsoft Active Director Topology Diagrammer. AD Diagrammer eli ”ADMap” on nykyään asiakkaiden vapaasti ladattavissa. ADMap tuottaa kuvauksen suoraan Visio- ohjelmalle (jonka pitää olla käynnissä diagnostikka-työasemassa).

<http://www.microsoft.com/downloads/details.aspx?familyid0cb42fc06-50c7-47ed-a65c-862661742764&displaylang=eng>

### **7.2 Sähköpostilaatikoiden määrä**

Sähköpostilaatikoiden määrä Teachers Training Collegella:

- Dong Ha noin 200 käyttäjää
- Muut toimipisteet noin 100 käyttäjää

Näin ollen esimerkiksi massamuistien käytön mitoituksissa sähköpostilaatikoiden kokonaismääräksi on arvioitu noin 300.

### **7.3 Postilaatikoiden kokorajoitus**

Tällä hetkellä sähköpostilaatikoiden koko on noin 80%:lla käyttäjistä 300MB, loput ovat 300MB-2GB. Mitoituksissa käytettävän sähköpostilaatikon koko on 600MB. Teachers Training Collegen konesalissa on käytettävissä nopea SAN -massamuisti järjestelmä.

### **7.4 Sähköpostipalveluiden sijoituspaikka**

Sähköpostipalvelinten sijoituspaikka tulee olemaan Teachers Training Collegen konesali Dong

Ha. ”Fyysisiä” toimipisteitä Teachers Training Collegella on kolme. Nämä ovat jakautuneet ympäri Dong Ha:n kaupunkia. Dong Ha:n pääpaikassa on noin 200 käyttäjää.

## **7.5 Sähköpostiliikenteen reititykset**

Kaikki sähköpostiliikenne reititetään ulkomaailmaan päätoimipisteen kautta. Tämä yksinkertaistaa huomattavasti migraatioita. Sähköpostin reitityksen takia on erityisen tärkeää, että toimipisteiden aliverkkomääritykset (subnet) ovat kunnossa. Exchange 2007 käyttää sähköpostien reitittämiseen vanhoja routing group -määritysten sijaan AD toimipisteitä.

## **7.6 Työasemat**

Tällä hetkellä on käytössä Office 2003, SP3-päivitys on vielä meneillään. Office 2007:n päivitysajankohdaksi on arvioitu ”samaan aikaan kuin Windows XP SP3”. Todennäköisesti ainakin päätoimipiste sähköpostijärjestelmä päivitetään vuoden kuluessa.

Työasemien uusiminen on meneillään. Jokaiseen työasemaan pyritään saamaan 2GB keskusmuistia.

Noin 80%:a käyttäjistä käyttää kiinteitä työasemia. Näiden Outlook 2003- ohjelmat ovat ns. Online-toimintatilassa. Estettä cached -toimintatilaan siirtymiselle ei ole.



## **8.1 Edge Transport Server**

Edge Transport servereiden kautta kulkee Exchange 2007-järjestelmän SMTP -sähköpostit sisään ja ulos. Edge Transport -serverissä tutkitaan sähköpostit virusten varalta ja suodatetaan roskaposteja. Edge transport-palvelimet eivät ole toimialueen jäseniä. Edge -palvelinten kuormantasaus hoidetaan DNS Round Robin-tekniikalla.

## **8.2 HUB transport Server**

Hub Transport serverit toimivat välittäjinä SMTP yhdyskäytäväpalvelinten ja Exchange 2007 - Mailbox palvelinten välillä. Hub Transport-palvelimet tasaavat kuormitusta automaattisesti eli niille ei laiteta Network Load Balancingia-NLB:tä.

Hub Transport-palvelimet siirtävät myös tietoa mailbox-palvelinten sähköpostilaatikoiden välillä. Hub Transport-palvelimet ovat toimialueen jäseniä. Mikäli sähköpostiliikennettä halutaan tarkkailla, sitä tehdään usein nimenomaan HUB Transport-palvelimilla.

## **8.3 Client Access Server**

Etäkäyttäjät kytkeytyvät Exchange 2007 -sähköpostipalveluihin Client Access palvelimen avulla. Etäkäyttäjillä voi olla ohjelmistona Outlook (Outlook Anywhere-RPC over http), www-selain (Outlook Web Access) tai mobiililaitteissa ActiveSync (erikoistapauksissa myös POP-3 tai IMAP4-sähköpostiohjelma, joskaan tätä ei suositella tietoturvasyistä ainakaan ilman salausta).

Myös sisäverkon Outlook Web Access -käyttäjät ja kalenterivaroituksia tekevät käyttäjät kytkeytyvät Client Access Server-palvelimiin, Client Access-palvelimet ovat myös toimialueen jäseninä ja ne kannattaa laittaa NLB -klusteriin

## 8.4 Mailbox Server

Sähköpostipalvelimet säilyttävät käyttäjien postilaatikot ns. storage group –tietovarastojen mailbox-tietokannoissa. Mailbox-palvelimet eivät itse lähetä tai vastaanota tietoja, vaan niiltä haetaan ja tuodaan sähköpostiviestejä. Sisäverkon Outlook-käyttäjät kytkeytyvät suoraan Mailbox-palvelimiin paitsi Outlook Web Accessia käyttäessään tai tehdessään kalenterivaroituksia (free-busy). Mailbox-palvelimet ovat luonnollisesti toimialueen jäseniä.

## 8.5 Skaalautuvuus

Exchange 2007-ympäristö skaalautuu tarvittaessa joka kohdastaan. Uusia Mailbox-, Hub-, Transport-, Client Access ja Edge-palvelimia voidaan lisätä tarvittaviin kohtiin yksinkertaisella prosessilla.

Tärkeä sähköpostijärjestelmän kuormitukseen vaikuttava tekijä on yhtäaikaisten käyttäjien määrä sisäverkon ja etäkäytön palveluissa sekä tulevien ja lähtevien sähköpostien määrät ja viestien koot. Mailbox-palvelinten mitoitus vaikuttavat sähköpostilaatikoiden maksimikoot, keskimääräiset täyttöasteet ja vaadittavat sähköpostiviestien palautusajat varakopioilta. Lisäksi vaikuttaa se, kuinka kauan tuhotut sähköpostiviestit säilytetään käyttäjän ”poistetut-kansiossa” (yleinen käytetty aika on 14 päivää).

Lisäksi on syytä huomata, että erittäin suurten, esim. gigatavun sähköpostilaatikoiden kanssa ei kannattane käyttää Outlook ns. Cached modea eli kyseisen käyttäjän järjestelmälle aiheuttama kuormitus kasvaa selvästi. Normaalien maksimissaan muutaman sadan megatavun sähköpostilaatikoiden kanssa kannattaa ehdottomasta käyttää cached-moodia!

## 8.6 Tietoturva

Exchange 2007-ympäristön tietoturva koostuu mm. Active Directorin ja Exchange-palveluiden, verkon tietoliikenne palveluiden, työasemien ja mobiililaitteiden tietoturvasta, virustorjunnasta ja spam-torjunnasta.. Myös nykyaikaisten tekniikoiden kuten etäkäytön, langattomien verkkojen,

toimikorttien jne. vaikutus tietoturvaan on otettava huomioon Exchange-ympäristöjen suunnittelussa.

Exchange 2007 –sähköpostijärjestelmä tarvitsee nopean ja luotettavan yhteyden ns.Global Gatalog-palvelimiin,joita on syytä olla korkean käytettävyyden takaamiseksi vähintään 2. DC-palvelinten operointiin ja diagnostiikkaan on kiinnitettävä erityistä huomiota myös Exchangen takia.

Kaikkiin Exchange 2007-palvelimiin tultaneen asentamaan virustorjunta-ohjelmisto lukuun ottamatta Client Acces Server-palvelimia.

Exchange 2007 –infrastruktuurin tietoturvaa parantaa merkittävästi se, että Exchange-palvelinrooleja asennettaessa kyseiseen palvelimeen asennetaan vain kyseisen roolin tarvitsemat ohjelmat, ei mitään ylimääräistä.

Sähköpostijärjestelmän tietoturvan ja korkean käytettävyyden osalta noudatetaan luonnollisesti sovittuja tietoturvasuosituksia ja –käytäntöjä.

## 9. Exchange 2007 –infrastruktuurin lokit

Exchange 2007 –ympäristöstä on mahdollista saada monenlaisia lokeja ja raportteja. Lokituksen määrää ja laajuutta voidaan säätää voimakkaasti.

Käyttöjärjestelmän tapahtumalokeihin (event log) tallentuvia ilmoituksia voidaan säätää Exchangen kaltaisissa sovelluksissa. Lokien luonne vaihtelee sen mukaan, missä roolissa (tai rooleissa) toimiva Exchange 2007-palvelin on kyseessä (edge, client acces, hub, mailbox).

Exchange-palvelinten lisäksi sähköpostin-infrastruktuurissa ovat voimakkaasti mukana toimialueen hallintakoneet (DC) Global Catalog -hakemistoineen sekä tietenkin nimenselvitykseen osallistuvat DNS-palvelimet.

Exchange-palveluiden toiminnan kannalta tärkeää on Internet Information Services (IIS) -palveluiden toimivuus. IIS-palveluilla on omat lokinsa ja ne tuottavat ilmoituksia myös käyttöjärjestelmän tapahtumalokeihin.

Exchangessa on oma, viestiliikennettä seuraava ”message tracking log”-järjestelmä. Tämän järjestelmän kautta saatavat tiedot on syytä määritellä erityisen huolellisesti koska ”message tracking log” -järjestelmä mahdollistaa laajimmillaan käyttäjien sähköpostiliikenteen täydellisen seuraamisen.

## 10. Exchange 2007 –ympäristön asentaminen

Tässä luvussa kuvataan Exchange 2007 –infrastruktuurin asentaminen, mukaan lukien CCR-klusterin asentaminen ja konfiguroiminen.

Sähköpostipalveluiden konfigurointi pitää sisällään Exchange 2007 –palvelinten peruskonfigurointien lisäksi suuren joukon asioita, jotka pitää ottaa huomioon uutta Exchange 2007 –ympäristöä suunniteltaessa, testiympäristöä rakennettaessa ja testatessa ja tuotantoympäristöä pystytettäessä.

Sähköpostikannat ja niiden tapahtumalokit vievät joka tapauksessa tuotantoympäristössä niin paljon levyosioita (kanta+tapahtumalokit), etteivät levykirjaimet riitä. Näin ollen jo kevyeseen testiympäristöön laitetaan Exchange 2007:n storage groupit, storet ja tapahtumalokit mount point -resursseiksi.

### 10.1 WINS-palveluiden tarve

Suunniteltuun Exchange 2007 –infrastruktuuriin on suositeltavaa perustaa WINS-palvelu, vähintäänkin tarvittaessa nopeasti päälle kytkettävänä vararatkaisuna. Mikäli WINS on päällä vararatkaisuna, niin on syytä tarkkailla, kuinka usein nimenselvennys siirtyy vararatkaisun varaan.

- Exchange 2007:ää vanhempien Exchange-versioiden kuten Exchange 2003 migraation aikana/kanssa on ehdottomasti syytä käyttää WINS-palvelua
- Exchange 2007-ympäristössäkin käytetään Windows-klusterointia (MS Clustering Sercvice-MSCS) Windows 2003 –käyttöjärjestelmässä, jolloin WINS on suosituksena.
- Mikäli WINS päätetään laittaa sähköpostin infrastruktuuriin, niin kannattaa tarkkailla huolellisesti minkä verran WINS-palvelua käytetään DNS-nimenselvityksen sijaan (failover)



## 10.2 PKI-diagnostiikka

Exchange 2007 –ympäristöön kuuluvat oleellisena osana hyvin toimivat PKI-palvelut. Seuraavista käskyistä ja toimivasta PKI-infrastruktuurin käytöstä luodaan ns. baselane, jonka perusteella voidaan arvioida PKI:n toimivuutta jatkossa

- Certutil (ilman parametrejä CA-palvelimen tunnustiedot)
- Certutil –cainfo (PKI-palveluiden tilatietoja)
- Certutil –verifykeys (CA-palvelin on kunnossa varmisteidensa osalta)
- Certutil –f –dspublish ”X.crt” RootCA (CA-palvelinten NetBIOS-nimi, julkaistaan varmenne ja sen sulkulista AD:hen –voidaan tarkistaa, onko jo julkaistu X.crt ha \*.crl)
- certutil –addstore –f Root ”crt ja crl” (voidaan lisätä varmenteet ja sulkulistat paikallisesti ja tarkistaa, että varmenne ja sulkulista löytyvät paikallisesti tietyltä palvelimelta)
- Lisäksi tarkistetaan CA –ohjelmalla (MMC-snap-in), että palvelun ominaisuudet ovat kunnossa, mistä löytyvät sulkulistat jne.)
- Certutil –URL ”Cert.cer” (voidaan tarkistaa varmenteeseen liittyviä ominaisuuksia kuten CRL-polkuja ja sitä, että polut jne. toimivat)
- Certifical –gtreg cs\crl\* (voidaan tarkistaa CRL-listojen polkuja ym. asetuksia)
- Certutil –getreg ca \vali\* (voidaan tarkistaa varmenninpalvelimen varmenteen voimassaoloaika)
- Huom. CA-palvelimeen yhteyttä otettaessa on syytä avata portit 80, 443 ja 135

## 10.3 Exchange 2007 –sähköpostipalvelinten levyjen valmisteleminen –diskpart

Exchange 2007 –levyt on syytä alustaa diskpart ohjelmalla.

Windows Server 2003 –käyttöjärjestelmän suositus on ollut ja on edelleen aling=64 (eli 64 kilotavua) Windows Server 2008 –käyttöjärjestelmä asentaa automaattisesti aling=1024 (eli yhden megatavun -tätä ei tarvitse Windows Server 2008:ssa asentaa käsin).

Kannattaa myös tarkistaa suositus laitevalmistajalta. Levyvalmistajan suositus luonnollisesti on mahdollisesti poikkeavista arvoista määräävin.

Edellä kuvattu koskee kaikkia Exchange 2007-massamuisteja, eli oli kyseessä SAN-järjestelmä, RAID-levyt tai yksittäiset kiintolevyt.

Ns. signaturea ei tarvitse kirjoittaa levyille Disk Management-ohjelmalla ennen diskpart ohjelman käyttämistä.

Diskpart-käskyjä ovat:

- list disk
- select disk 1
- detail disk
- create partition primary align=1024
- assign mount=c:\mountpoints\CMS01sg01Data
- list disk
- sitten format-käsky jossa allocation unit size on
- kannoille 64 kb
- lokeille 4kb (format ohjelmassa 4096 (tavua))  
... ellei massamuistivalmistaja toisin suosittele

#### 10.4 Edellytykset Exchange 2007:n asentamiseksi

Seuraavat esivalmistelut tehdään kaikille Exchange 2007:n palvelimille

- .NET Framework 2.0 (ja .NET Framework SP1)
- MMC 3.0 (löytyy valmiina Windows Server 2003 SP2 R2:sta)(tai KB907265)
- Powershell 1.0 –komentotulkki  
(<http://www.microsoft.com/windowsserver2003/technologies/management/powershell/download.aspx>) b
- Microsoft Core XML Services (MSXML) 6.0  
(<http://www.microsoft.com/downloads/details.aspx?FamilyID=993C0BCF-3BCF-4009->

[BE21-27E85E1857B1&displaylang=en](#)) c

- Support Tools (huom. oikea käyttöjärjestelmäversio – ja oikea “bittisyys”!)
- Hotfix korjaukset (kuten tarvittaessa KB926776)
- Time zone update –hotfix (KB931836) –kaikkiin Exchange-palvelimiin.
- Palvelinten oltava ajan tasalla myös mm. Exchangen hotfix-päivitysten ja ns. Update Rollup –päivitysten suhteen.
  - o Asennetaan kaikkiin Exchange 2007 SP 1 –palvelimiin
  - o Update Rollup 5 for Exchange 2007 SP1  
(<http://msexchangeteam.com/archive/2008/11/21/450151.aspx>) d
  - o tarkista, että Exchange 2007 –palvelimet ovat varmasti asennettu SP1 tasolle
    - Oikea versio on 08.01.0240.006 usein esitetään myös muodossa Version 8.1 (Build 240.6)
- AD:N valmistelemineen
  - o Asennetaan GPMC ja ajetaan ”skripti”
  - o Asennetaan GPMC eli Group Policy Management Console – ohjelmisto. Siirrytään hakemistoon C:\program files\gpmc\scripst. Aketaan seuraava komento:cscript grantpermissiononallgpos.wsf ”Enterprise Domain Controllers” /permission:read /domain: jokin.vn
  - o setup /PrepareLegacy/ExchangePermissions
    - vain mikäli ollaan tekemässä Exchange 2003-> Exchange 2007 migraatiota
  - o vaatii powershell 1.0
  - o mikäli IT-ympäristöissä on (hyvin) hitaita ja epävarmoja verkkoja niin seuraavien käskyjen välissä kannattaa odottaa esimerkiksi vuorokauden verran
- Setup /PrepareScema
- Setup /PrepareAD/OrganizationName:Organisaatio
  - o Synnyttää käyttäjäryhmät
    - Exchange Organization Administrators
    - Exchange Recipient Administrators
    - Exchange View-Only Administrators
    - Exchange Servers
    - ExchangeLegacyInterop
  - o setup /PrepareDomain –edellisen kolmen ajon lisäksi suoritetaan jokaisessa mahdollisessa alitoimialueessa.

- how to Prepare Active Directory and Domains:

<http://technet.microsoft.com/en-us/library/bb125224.aspx> e

- resurssipostilaatikko "off-linenena"

## 10.5 Palvelininfrastruktuurin valmisteleminen

- Regedit ohjelmalla

- HKLM->System->CurrentControlSet->Services->TCPIP->Parameters

- TcpTimedWaitDelay: 60 (sekuntia, Dword, desimaalisena)

- MaxUserPort: 65535 (Dword, desimaalisena)

- HKLM->System->CurrentControlSet->Services->W32Time->Parameters

- "DC01"-palvelimessa Type-valuen tulee olla "NTP", \*kaikissa muissa\* palvelimissa tulee Type-valuen olla "NT5DS"

- "DC01"-palvelimessa

- w32tm/config/manualpeerlist:"ntp.domain.vn"

- /syncformflags:manual/reliable:yes /update

- w32tm /config /update

- w32tm /stripchart /computer:"ntp.doamin.vn"/samples:3 /dataonly

- Optio: mikäli esim NAT-tietoliikenteessä on huolia, voidaan määritellä

- EnableRSS->0

- EnableTCPA->0

- EnableTCOChmney->0

## 10.6 Tietoliikenteen reititykset -default gateway

Perussääntö default gateway – eli oletusreitimmäärityksiä tehtäessä on, että dgw:t määritellään osoittamaan "ulospäin" organisaation verkosta-"external-", "internet-", "perimeter"-verkkoihin.

Mikäli sisäverkon arkkitehtuuri on kovin monimutkainen, käytetään hallintaverkkoja (maintenance) tai halutaan varmistaa ns. paluupakettien reitittyminen takaisin yhteyttä ottavalle

koneelle. Käytetään ns. permanent route-määrittelyitä (route add -p...)

Mihinkään palvelimeen –tai työasemaan ei jätetä määrittelyksi kahta default gatewayta. Seuraava teksti on Microsoftin KB-artikkelista:

”Only one default gateway should be configured on any multihomed computer. The default gateway is global configuration for the server, not a setting that must be set for each network adapter. The server is already aware of all the networks it is directly connected to, and adds a route to each network for which it has a TCP/IP address. “

Luettavissa: <http://support.microsoft.com/kb/157025> Luettu 3.5.2009

## 10.7 CAS-palvelinten asentaminen

- Yleiset esivaatimukset
- On erittäin tärkeää, että CAS-palvelimessa on vähintään 2 verkkoliitäntää eli network interfacea
  - o Nämä ovat ”ulkoverkko” ja ”sisäverkko” ja niiden lisäksi mahdollinen hallintaverkon liittymä.
- Tarkistetaan, että kello on oikeassa ajassa ja personal firewall on pois päältä
- Nimetään verkkoliitännät ja tarkistetaan niiden binding-järjestys (“public” on ylimmäisenä)
- Liitetään palvelimet toimialueeseen
- Asennetaan ASP.NET ja Network COM+, IIS, WWW
- Enable ASP.NET 2.0/64-bit (script binding) (<http://support.microsoft.com/kb/894435>)
- f
- Asennetaan RPC over HTTP Proxy (windows components->networking services)
- Setup /mode:install /roles:CA
- Verifioidaan get-ExchangeServer
- Loki: c:\ExchangeSetupLogs\ExchangeSetup.log
- Muut klustereiden tarkistukset on kuvattu omassa kohdassaan

Toinen CAS-palvelin asennetaan ns. NLB-klusteriin ensimmäisen CAS-palvelimes kanssa.

## 10.8 Hub-palvelimen asentaminen

- Yleiset esivaatimukset (.NET Framework 2.0, Support Tools, hotfixit jne)
- Liitetään toimialueeseen (ajan varmistamisen, DNS-palvelun konfiguroimisen ym. jälkeen).
- Asennetaan MMC 3, PowerShell, .NET 2.0 update KB926776 mikäli tarvitaan (<http://go.microsoft.com/fwlink/?linkid=74465>). g
- IIS:n asentaminen Hub- palvelimeen kannattaa tehdä, koska tällöin Hub-palvelimen Exchange Management Consolella voidaan myös hallita CAS palvelimia.
  - o Asennetaan ASP.NET ja Network Com+, IIS, WWW.
  - o Enable ASP.NET 2.0 /64-bit (script binding) (<http://support.microsoft.com/kb/894435>) h
  - o Setup /mode:install /roles:HT
  - o Verifioidaan get-ExchangeServer
  - o Loki: c:\ExchangeSetupLogs\ExchangeSetup.log

Toisen Hub-palvelimen asentaminen on ensimmäisen palvelimen asentamisen jälkeen helppoa. Edelläkuvatut toimenpiteet toistetaan toisella palvelimella. Palvelimet alkavat tasata kuormaa automaattisesti.

### 10.8.1 Sähköpostin ”ulkoiset” reititykset Hub-palvelimella

Jos ei käytetä Edge Transport-palvelimia, on Hub Transport palvelimille määriteltävä seuraavat asiat. Olen kuitenkin ajatellut laittaa tähän suunnitelmaan mukaan myös Edge-palvelimet. Tällöin tämän kappaleen tiedot ovat ainoastaan ”varmuuden vuoksi”. Lisäksi vaikka infrastruktuurin sisäiset connectorit syntyvätkin automaattisesti, on hyvä tietää miten niitä konfiguroidaan tarvittaessa.

Hub-palvelinten TCP/IP-määrittelyyn tulee tehdä rajoitus, että Hub-palvelimet keskustelevat vain SMTP-gatewayn palvelinten (IP-osoitteet tai nimet) kanssa. SMTP-palvelinten lisäksi saatetaan joutua sallimaan vanhojen sähköpostityöasemaohjelmien sähköpostien lähettäminen Hub-palvelinten välityksellä SMTP-S-protokollan avulla. Hub-palvelimen ns. receive-connectoriin

konfiguroidaan anonymous relay-palvelu.

- ("To Use the Exchange Management Shell to create a new Receive connector that grants permission to anonymous connections")
- `New-ReceiveConnector-Name <Name>-Usage Custom-PermissionGroups AnonymousUser -Bindings <LocalIPAddress:25> -RemoteHelpRanges<SourceServer>`
- Esimerkkikäsky: `New-ReceiveConnector -name "Anonymous Relay" -Usage Custom -PermissionGroups AnonymousUser -Bindings 0.0.0.0:25 -RemoteRanges 192.168.6.77`
  - 0.0.0.0 tarkoittaa kaikkia palvelimen paikallisia IP -osoitteita (sähköposteja voidaan ottaa kaikkien verkkoliitännöiden kautta)
  - Huom. palvelimen tietoliikenneasetuksesta on rajoitettava ne IP-osoitteet, joiden kanssa palvelin suostuu viestimään.
- Mikäli luodun ReceiveConnectorin asetuksia halutaan muuttaa, se käy `Set-ReceiveConnector -cmdlet` ohjelmalla
- sitten vielä: `Get-ReceiveConnector "Anonymous Relay" | Add-ADPermissions -User "NT AUTHORITY\ANONYMOUS LOGON"-ExtendedRights "Ms-Exch-SMTP-Accept-Any-Recipient"`
- Huom. receive-konnektorit eivät replikoidu Hub-palvelinten välillä (send-konnektorit replikoituvat)
- [http://technet.microsoft.com/en-us/library/bb232021\(EXCHG.80\).aspx](http://technet.microsoft.com/en-us/library/bb232021(EXCHG.80).aspx) i

- Toinen vaihtoehto on konfiguroida ns. externally secured -konnektori (tämä edellyttää esim. IPSec-autentikoinnin käyttämistä)

- Tiivistettynä tämä toinen vaihtoehto: "The messages that originate from the specified IP addresses are treated as authenticated messages. The message bypass anti-spam checks, bypass message size limit checks, and can resolve anonymous senders. The disadvantage of this strategy is the remote IP addresses are considered completely trustworthy. The Permissions that are granted to the remote IP addresses allow the remote messaging server to submit message as if they originated from internal senders within your exchange organization (<http://technet.microsoft.com>) ;
- Tulkinta: "adding an additional filtering layer after SMTP gateway may not be

possible. Mail relay from “internet” may not considered “completely Trustworthy” by security people”

- Hub-palvelimen ns. send-konnektoriin on konfiguroitava smarthost palvelimen tai SMTP-gateway palvelimen osoite.

- o Esimerkkikäsky: New-SenderConnector –Name ”Subsidiary Send Connector” – Usage Custom AddressSpace ”\*.contoso.com;5”, ”\*fabrikam.com;8” – DnsRoutingEnabled \$false –SmartHosts 192.168.1.20 –MaxMessageSize 20MB
- o Puolipisteellä erotetut luvut ovat prioriteettejä.
- o Mikäli luodun SendConnectorin asetuksia halutaan muuttaa, se käy Set-ReceiveConnector –cmdlet ohjelmalla

Mm. seuraavat Technet-artikkelit kuvaavat tämän kappaleen konfigurointeja.

[http://technet.microsoft.com/en-us/library/bb738161\(EXCG.80\).aspx](http://technet.microsoft.com/en-us/library/bb738161(EXCG.80).aspx) k

[http://technet.microsoft.com/en-us/library/bb232021\(EXCG.80\).aspx](http://technet.microsoft.com/en-us/library/bb232021(EXCG.80).aspx) l

[http://technet.microsoft.com/en-us/library/aa998836\(EXCG.80\).aspx](http://technet.microsoft.com/en-us/library/aa998836(EXCG.80).aspx) m

[http://technet.microsoft.com/en-us/library/aa998294\(EXCG.80\).aspx](http://technet.microsoft.com/en-us/library/aa998294(EXCG.80).aspx) n

## 10.9 Sähköpostin ”sisäiset reititykset koulujen välillä

Exchange 2007 SP1 käyttää järjestelmän sähköpostien sisäverkon reitityksiin pätevät seuraavat säännöt.

- Exchange 2007 käyttää AD toimipisteitä reititessään sähköposteja organisaation sisäverkossa.
  - o Exchange 2007 kunnioittaa IP site link cost –kustannuksia ym. arvioidessaan sähköpostin oikeita kulkureittejä.
  - o Kun organisaatiolla kuten Teachers Training Collegella on selkeä keskustuimipiste (Dong Ha), niin Dong Ha voidaan määritellä ns. Exchange Hub –siteksi
    - sähköpostit pyritään tällöin ohjaamaan hub-toimipisteen kautta



- Exchange 2007:n asentaminen luo automaattisesti ns. routing group konnektorin –RGC. Exchange 2003- ja Exchange 2007 –ympäristöjen välille.
  - o Exchange 2003- ja Exchange 2007 –palvelinten välille on syytä määrittellä toisetkin bridgehead palvelimet
  - o Näin postin kulku eri ympäristöjen välillä ei ole yhden palvelimen varassa, etenkin jos Exchange versioita käytetään rinnakksin pitkään.
- Sähköpostiliikenteen optimoimiseksi saattaa kannattaa lisätä itse konnektoreja, mikäli joidenkin toimipisteiden välillä liikkuu paljon sähköposteja.
- Usean Exchange 2007 –sähköpostipalvelimia sisältävän toimipisteen käyttäminen ei edellytä mitään konfigurointeja Hub Transport –palvelimissa (ellei käytössä ole useita SMTP postidomaineja)
- Tämä tarkoittaa, että Hub palvelimelle ei ole ”välttämätöntä” tehdä mitään eli esim. tarvitse luoda uusia toimipisteiden välisiä organisaation infran sisäisiä konnektoreja (vaan asennettaessa automaattisesti syntyneet ns. impliittiset sisäiset konnektorit riittävät)
- jotta posti ylipäättään kulkisi ovat jotkin hienosäädöt usein tarpeellisia
- Tällöin AD toimipisterakenteen (topologia) on oltava erittäin hyvässä kunnossa ja tarkoituksen mukainen sähköpostiliikenteen kannalta.
- Kun Exchange 2007 –sähköpostipalvelut asennetaan Exchange 2003 –ympäristöön asennus luo näiden ympäristöjen välille automaattisesti send ja receive –konnektorit
- Kaikki Exchange 2007 –sähköpostipalvelimet ovat yhdessä ns. routing groupissa
- Kaikki Exchange 2007 –sähköpostipalvelimet ovat yhdessä ns. administrative groupissa

## 10.10 NDR -kuittausten käsitteleminen

Migraatioprosessin ajan Non-Delivey-Report eli NDR-raporttien on toimittava luotettavasti. Mikäli viestin lähettäjä ei saa NDR-raporttia, eikä viestiä löydy Koulun sähköpostijärjestelmästä, viesti tulkitaan helposti ”hävinneeksi”.

## 10.11 Edge -palvelinten asentaminen

Koululla on ollut aikaisemmin PostFix pohjaiset SMTP-gateway palvelimet. Exchange 2007 –päivityksen yhteydessä asennetaan uudet Edge-palvelimet.

Edge -palvelimen peruseriaatteita:

- Edge palvelimet ovat workgroupissa eivät toimialueen jäseninä (member server)
- Edge palvelinten kuorman taseus toteutetaan DNS round robinin avulla
- Edge palvelimet voivat tehokkaasti osallistua virus ja SPAM torjuntaan
- Sallitut toimialueet synkronoidaan Edge palvelimille kerran tunnissa
- Sallitut vastaanottajat synkronoidaan Edge –palvelimelle kerran 4 tunnissa.
- Synkronointi ja Edge välimuistin päivittyminen huomioon ottaminen vastaanottajan päivittyminen Edge palvelimille saattaa kestää 8 tuntia.
- Kun asennetaan Edge –palvelimia, kumpaankin palvelinta voidaan työstää yhtä aikaa rinnakkain.

Esi-Konfiguroinnit:

- Active Directory Application mode (ADAM) SP1  
(<http://www.microsoft.com/windowsserver2003/adam/default.mspx>) o
- .NET Framework 2 –SP1
  - o .NET 2 –päivitys KB926776 –tullee SP1:n mukana  
(<http://go.microsoft.com/?fwlinkid/=74465>) p
  - o Support tools
  - o MMC 3.0 –konsoli (KB907265) ellei ole jo valmiinna  
(<http://support.microsoft.com/kb/907265>) q
  - o PowerShell  
(<http://www.microsoft.com/windowsserver2003/technologies/management/powershell/download.mspx>) r
  - o Edge-palvelimet määritellään IP-asetuksista käyttämään sisäverkon DNS palvelimia (“AD01” ja “AD02” eli AD-integroidut palvelut)
  - o Edge –palvelinten DNS-suffikseiksi määritellään sisäverkon toimialue.
  - o Määritellään Edge-palvelinten nimet ja IP-osoitteet ulkoisiin nimipalveluihin

Asennus:

- Setup /mode:install /roles:ET
- Tarkistus: get-ExchangeServer
- Asennuksen lokit: c:\ExchangeSetupLogs\ExchangeSetup.log

Edge-palvelinten tarvitsemat portit:

- LDAP: Portti 50389/TCP
- Secure LDAP:Portti 50636/UDP
- SMTP:Portti 25/TCP

## 10.12 Edge-palvelinten konfiguroiminen

Luodaan ns. edge-subscription

- Huom. vanhenee 6 tunnissa, joten palomuurit on syytä konfiguroida ennen subscriptionin tekemistä.

Annetaan Edge –palvelimella –Exchange Management Shell:

```
-New-EdgeSubscription –FileName ”C:\EdgeSubscriptioninfo.xml”
```

- Kopioidaan syntynyt tiedosto Edge Transport palvelimelta Hub Transport –palvelimelle
- Subscription tiedosto kannattaa tuhota käytön jälkeen
- Asennetaan Edge-palvelimelle Exchange Management Shell
  - o Set-TransportServer –Identity ExEdge01 –ExternalDNSAdapterEnabled \$false – ExternalDNSServers <IP Address of DNS01>
- “pingataan” ristiin –Hub Transport palvelimelta Hub (FQDN-nimellä)
- Annetaan Hub-palvelimella –Exchange Management shelliin komento
  - o New-EdgeSubscription –filename ”C:\EdgeSubscriptioninfo.xml” – CreateInternetSendConnector \$true –site ”Default-First-Site-Name”
  - o Subscription tiedosto kannattaa tuhota käytön jälkeen

- Annetaan Hub-palvelimelta Exchange Management Shell
  - o New-AcceptedDomain -Name "ConsolidatedMessenger" - DomainName consolidatedmessenger.com -DomainType Authorative
    - Tämän cmdlet-käskyn avulla määritellään sähköpostille sallitut SMTP-domainnimet
  - o Replikoituvat automaattisesti Edge-palvelimille Edge-Subscriptionin yhteydessä
  - o Start-EdgeSynchronization
    - Käynnistetään konfiguraatietojen päivittäminen Edge-palvelimelle (Active Directory -hakemistopalvelusta)

### 10.13 CCR -mailbox palvelinten asentaminen

Esivaatimukset:

- Kussakin CCR-palvelimessa oltava vähintään 2 verkkoliitäntää eli network interfacea
  - o Nämä ovat "public" eli liittymä normaaliverkkoon ja "Heartbeat" eli CCR-node palvelinten välinen "private"-verkko
- Tarvitaan ainakin kaksi levyosiota (käyttöjärjestelmä, sivutustiedot ja mount-pointit sekä toinen osio sähköpostikantaa ja sen tapahtumalokeja varten)
  - o Huom Public Folder-palvelin (Offline Address Book -palvelin) on oltava erikseen.
    - Klusterin nodeihin ei voida sijoittaa muita Exchange 2007 -rooleja tai muita toimintoja kuten PF- tai OAB-palveluita
- Yleiset esivaatimukset (.NET Framework 2.0, support tools, hotfixit jne.)
- Liitetään toimialueeseen (aika, personal firewall, DNS-määritykset jne.)
- Luodaan cluster service account (ClusterAdmin)
- Tarkistetaan että private ja public-verkkoyhteydet ovat kunnossa (nimetään suurin prioriteetti/binding -public interfacelle) -verkkoyhteyksien palvelut (disabloidaan NetBIOS ja estetään DNS-rekisteröityminen private-yhteydeltä) jne.
- Asennetaan MNS-hotfix (<http://support.microsoft.com/?kbid=921181>) s
- Asennetaan Network Com+, IIS ja WWW node-palvelimiin
- Asennetaan MMC 3.0, PowerShell 1.0, tarvittaessa KB918980 (<http://www.microsoft.com/downloads/details.aspx?FamilyID0aa353712-05e7-4b08-888c->

[f8ecb998dc72\\$DisplayLang=en](http://go.microsoft.com/fwlink/?linkid=74465)) t ja .NET 2.0 –päivitys

(<http://go.microsoft.com/fwlink/?linkid=74465>) u

- Asennetaan KB918980, mikäli tarpeellista (todennäköisesti ei tarvitse asentaa erikseen)
- Asennetaan kaikki esivaatimukset myös klusterin tulevaan ”passiiviseen” nodeen
- Lisätään ClusterAdmin -> Exchange Organization Administrators- käyttäjäryhmään

#### 10.14 Asennetaan käyttöjärjestelmän perus-klusterointi

- cluster /create /wizard (luodaan klusteri)
- cluster /cluster:<ClusterName> /add /wizard (lisätään node 2 klusteriin)
- cluster group ja cluster group (siirretään perus-klusteriryhmä eli Cluster Group nodelta 1 nodelle 2 ja takaisin)
  
- Määritellään niin, että public-interfacen kautta voi mennä sekä ulkoinen, että heartbeat liikenne.
- Määritellään niin, että private-interfacen kautta voi mennä vain heartbeat liikenne
- klusterin sisällä määritellään niin, että private-liittymän prioriteetti on suurempi kuin public-liittymän prioriteetti (napautetaan hiiren oikealla näppäimellä klusterin nimeä jne)
- Määritellään Hub-palvelimelle ns.file share witness
- mkdir C:\MNS\_FSW\_DIR\_MBX01
- net share MNS\_FSW\_MBX01=C:\MNS\_FSW\_DIR\_MBX01  
/GRANT:Qttc\ClusterAdmin:F
- Cluster res “Majority node Set” /priv MNSFileShare=\\EXHUB01\MNS\_FSW\_MBX01
- Cluster group “Cluster Group” /move (aktivoidaan MNS-quorum siirtämälle se nodelta toiselle kaksi kertaa)
- Cluster croup ”Cluster Group” /move
- Cluster res ”MAjority Node Set” /priv (tarkistetaan quarum-määrittely)

## 10.15 Asennetaan CCR-klusterin aktiivinen “node”

- Määritellään hakemistot storage groupeille (järeämmässä testiympäristössä myös mount point –hakemistot)
  - o Storage-groupien, sähköpostikantojen ja lokitiedostojen tarvitsemat levyösiot kannattaa alustaa diskpart ohjelmalla.
  - o Mount pointit voidaan sijoittaa esim. hakemistoon C:\MountPoints
  - o StorageGroup: CMS01SG01DATA ja loki: CMS01SG01LOGS ja mailstore: CMS01SG01DB01
  - o “Aktiivinen” Exchange 2007 mailbox-palvelin voidaan asentaa kahdella tavalla.
    - setup.exe ohjelmalla graafisen käyttöliittymän kautta (jolloin Office 2003 – public-/system-folderit tulevat luoduksi automaattisesti
    - setup /mode:install /roles:MB /EnableLegacy/Outlook
    - Public Foldereita voidaan tutkia PFDAVAdmin.exe-ohjelman avulla
    - /EnableLegacyOutlook –valitsimella luodaan automaattisesti Outlook 2003:n vaatimat PF-system folder määrittymiset
    - Mikäli ei käytetä /EnableLegacyOutlook-valitsinta on PF storage group ja Public folder-tietokanta luotava käsin.
- Verifioidaan get-ExchangeServer
- Loki: c:\ExchangeSetuplogs\ExchangeSetup.log
- cd c:\Program Files\Microsoft\Exchange Server\bin
- ExSetup /newcms CMSname:EXCMS01  
/CMSIPAddress:<ClusteredMailboxServerIPAddress>
- Ensimmäinen storage group voidaan siirtää mount pointiin käskyllä
  - o Move-StorageGroupPath –identity;”EXCMS01\First Storage Group” – LogFolderPath: C:\Mountpoints\CMS01SG1Logs –SystemFolderPath: C:\MountPoints\CMS01SG1Logs –ConfigurationOnly \$true
- Ensimmäisen sähköpostitietokanta (Mailbox Database.edb) ja lokit voidaan siirtää explorerilla
  - o C:\Program Files\Microsoft\Exchange Server\Mailbox\First Storage Group -> C:\MountPoints\CMS01SG1Data
  - o Sitten voidaan antaa PowerShell komento
    - Move-DatabasePath –Identity: “E01\First Storage Group\Mailbox

Database” –EdbFilePath: “C:\MountPoints\CMS01SG1Data\Mailbox  
Database.edb” –ConfigurationOnly: \$true

- Exchange management Consolella voidaan määrittellä uudelle sähköpostitietokannalle “mount Database”
- Edellä olevat sähköpostin storage groupin, sähköpostikannan ja lokien siirtäminen kannattaa tehdä diagnostiikan takia- varsinaista käyttöä varten kannattaa kuitenkin luoda uudet kannat suoraan mount pointteihin
- Ensimmäinen storage group (nimeltään First Storage Group) ja sähköpostikanta (Mailbox Database) voidaan ja kannattaa tuhota
  - o ns system attendant mailbox luodaan tällöin automaattisesti toiseen sähköpostikantaan ja vastaava Active Directory –polku (configuration ->services ->Microsoft Exchange ->organisatio ->administrative group ->Servers ->CMS01 (cluster mailbox server- virtuaalikone) ->Microsoft System Attendant ->properties ->homeMDB) päivittyy myös automaattisesti viittaamaan tähän uuteen kantaan
  - o First Storage Groupin ja Mailbox Databasen tuhoamisen jälkeen uudelleenkäynnistetään (restart) system attendant-palvelu (service)
  - o Katsotaan ADSIEdit-ohjelmalla, mihin sähköpostikantaan järjestelmä perustaa uuden System Attendant –sähköpostilaatikon
    - Kyseinen sähköpostitietokanta ”mountataan” ja ”dismountataan”, jolloin järjestelmä luo ko. kantaan System Attendant –sähköpostilaatikon
  - o Nyt uuden CCR-sähköpostiklusterin aktiivinen node on valmis

#### 10.16 Asennetaan CCR-Klusterin passiivinen ”node”

- Luodaan ”passiivisen” klusterin noden c-levylle hakemisto C:\MountPoint ja kaksi levyosiota store ja log-tiedostoille (CMS01SG1Data ja CMS01SG1Logs).
- Mountataan Data- ja Logs-osiot mount pointiin
- ”Passiivinen” Exchange 2007 mailbox-palvelin voidaan asentaa kahdella tavalla
  - o Setup.exe-ohjelmalla graafisen käyttöliittymän kautta (jolloin Office 2003 – public/system-folderit tulevat luoduksi automaattisesti)
  - o setup /mode:install /roles:MB

- o Get-StorageGroupCopyStatus (tutkitaan että klusteri alkaa toimia kunnolla)
- o Move-ClusteredMailboxServer –Identity EXCMS001 ja toisen kerran Move-ClusteredMailboxServer –Identity EXCMS001 eli siirretään klusteroitu virtuaalinen sähköpostipalvelin node 1:ltä node 2:lle ja takaisin
  - mikäli Move\_ClusteredMailboxServer-käskey epäonnistuu, storage group voidaan elvyttää käskyllä
  - Restore-StorageGroupCopy –Identity <StorageGroupIdParameter> [-Confirm [<SwitchParameter>]] [DomainController <Fqdn>] [-Force<SwitchParameter>] [-ReplaceLocations <SwitchParameter>] [-StandbyMachine <String>] [-Whatif [<SwitchParameter>]]
- Tämän jälkeen voidaan vielä määrittellä Hub-palvelimella sijaitsevan dumpster-varaston toimintaparametrit ja itse klusterin failover-parametrit

### 10.17 Sähköpostiklusterin palvelut -käynnistysjärjestys

Klusterin palvelut tulevat päälle seuraavassa järjestyksessä

- Klusterin IP-resurssit
- Klusterin nimi (Cluster Name-MailCluster)
- Sähköpostiklusterin (CMS) IP-osoite
- Sähköpostiklusterin nimi (NetworkName)
- Exchange Information Store Instance
- Storage Groupit /Mailstoret
- Exchange System Attendant

### 10.18 Konfiguroidaan Client Access –palvelin tehtäviinsä

- Mikäli käytetään POP tai IMAP-protokolia, ne enabloidaan seuraavasti
  - o Set-service msExchangePOP3 –startuptype automatic
  - o Set-service msExchangeIMAP4 –startuptype automatic
  - o Start-service msExchangePOP3
  - o Start-service msExchangeIMAP4



- Konfiguroidaan OWA:a varten forms based -autentikointi ja tarvittaessa UPN-logon
  - o Set-owavirtualdirectory –identity ”owa (default Web site)” –FormsAuthentication:1 –LogonFormat PrincipalName
  - o Annetaan IISRESET
  - o Aktivoidaan outlook anywhere (RPC over HTTP) –palvelu
    - Exchange Management Console->server configurations ->client access->actions/enable outlook anywhere (basic authentication)
- Konfiguroidaan autodiscovery palvelu (tarvittaessa autodiscoverredirect:iin avulla)
- Uusi hakemisto voidaan varmistaa Get-AutodiscoverVirtualDirectory
- Autodiscovery palveluita ja AutoConfiguration toiminnallisuutta voidaan kätevästi testata Outlook 2007.n avulla pitämällä alhaalla control näppäintä ja napauttamalla ruudun alalaidasta (taskbar) hiiren oikealla näppäimellä outlook kuvaketta
  - o tällöin käynnistyy ”Test E-mail AutoConfiguration”-ohjelma, joka kertoo konfiguraation eli käytettävät we-osoitteet jne.
  - o OAB kuntoon
  - o Set-OABVirtualDirectory –identity ”EXCAS001\OAB (Default Web Site)” –externalurl <https://webmail.qtttc.vn/OAB> -RequireSSL:\$true
  - o Ulkoiset osoitteet kuntoon
  - o Set-WebServicesVirtualDirectory –identity “EXCAS001\EWS (Default Web Site)” –externalurl <https://webmail.qtttc.vn/EWS/Exchange.aspx> -BasicAuthentication:\$True

## 10.19 Rakennetaan Network Load Balancing CAS-palvelimelle

Network Load Balancing määritellään seuraavasti

- mennään verkkokortin asetuksiin
- General->Network Load Balancing päälle->properties
- Cluster Parameters IP+Subnet Mask + Full Internet name +Unicast
- Host Parameters priority 1 + Dedicated IP + subnet mask + started port rules – tarkistetaan ei muutoksia
- Lisätään klusterin VIP-IP osoite perus-TCP-IP asetuksiin

- NLB-klusterin VIP osoite täytyy konfiguroida käsin kummankin noden perus ip-asetuksiin
- Käynnistetään Network Load Balancing Manager
- mennään cluster properties
- Lisätään toinen ip osoite NLB klusteriin
- Vaihdetaan klusterin ensimmäinen VIP-IP osoite Autodiscover-web-sitelle
- Vaihdetaan toinen klusterin VIP-IP osoite AutodiscoverRedirect-web-sitelle
- Pidetään huolta, että uudet VIP-IP\_ osoitteet löytyvät nimipalvelusta
- CAS-palvelimilla on kaiken kaikkiaan 4 VIP-IP-osoitetta eri palveluita varten
- tarkistetaan vielä lopuksi että klusterin nodeissa perus-TCP-IP-osoitteissa (Advanced TCP/IP Settings näyttää kaikki IP-osoitteet) ovat mukana sekä host-dedicated-osoitteet että kaikki VIP-IP-osoitteet

Perustietoa:

<http://support.microsoft.com/kb/323431> w

## 10.20 Client Access –palvelinten varmenteiden käsitteleminen

- Varmenteen hakeminen CAS-palveluille
  - o Varmenne CAS-palveluille
    - New-ExchangeCertificate –generaltesrequest –PrivateKeyExportable \$true- subjectname ”dc=vn,dc=qtttc, o=qtttc DCorporation ,cn=webmail.qtttc.vn” –domainname EXCAS001,EXCAS001.qtttc.vn,webmail.qtttc.vn,qtttc.vn,smtp.qtttc.vn –path c:\EXCAS001\_certreg.txt
    - Varmenteen testaaminen
    - Get-ExchangeCertificate | fl subject.issuer.services.thumprint
    - Myös yksityinen avain syytä ottaa talteen “privatekey määrittäminen-avulla; yksityinen avain tarvitaan, mikäli palvelu julkistetaan palomuurissa joka osaa päättää käyttäjän SSL yhteyden ja avata uuden SSL yhteyden varsinaiseen palveluun
    - [http://technet.microsoft.com/en-us/library/aa998327\(EXCHG.80\).aspx](http://technet.microsoft.com/en-us/library/aa998327(EXCHG.80).aspx) x
- otetaan varmenne Exchange käyttöön

- Import-ExchangeCertificate -path <certificate\_file\_name>.cer -friendlyname "Teachers EXCASTC01"
- Otetaan tämän käskyn tuottama "thumbprint" talteen copy-paste käskyllä ja sijoitetaan se seuraavaan käskyn <certificate-thumbprint> -parametrin paikalle
- kiinnitetään Exchange käyttöön otettu varmenne palveluihin
- Enable ExchangeCertificate -thumbprint <certificate-thmprint> -services "IIS,POP,IMAP"
- Mikäli halutaan ottaa palvelut pois varmenteelta (tai vaihtaa varmennetta) – tuhotaan vanha varmenne ja otetaan käyttöön uusi varmenne; palveluiden ottaminen pois varmenteelta ei tee ei itseasiassa päivityä ns metabase-määrittäjiä
- Web sivusto RCP over http konfiguroinnille ja ohjeet sen käyttämiseen
  - kyseisestä web sivustosta voidaan ladata PRF -profiilit outlook ohjelmille sähköpostipalveluun kytkeytymistä varten
  - Suunniteltava Offline Address Book –osoitekirjojen kopioiminen OAB palvelimelle

## 10.21 Tarkistetaan Exchange-palvelinten konfiguraatiot

Exchange 2007 palvelinten konfiguraatiot voidaan tarkistaa perusteellisesti ExBPA eli Exchange Best Practices Analyzer ohjelmalla. Ohjelma kertoo virheilmoitusten ja varoitusten avulla mahdolliset ongelmat palvelinten konfiguraatioissa.

Konfiguraatioita, terveydentilaa tietoturvaa ja suorituskykyä ym. myös valvoa System center Operation Manager 2007 avulla.

## 10.22 Outlook Web Access –kutsu helpoksi

Tavoitteena on, ettei käyttäjien tarvitse kirjoittaa <https://palvelinnimi.toimialue.vn/owa>, vaan pelkkä <http://palvelin> tai <http://palvelin.toimialue.vn> riittää

Vaihtoehtoja määrittäminen toteuttamiseen on useita. Voidaan reitittää kaikki Default websiten

kutsut /QWA –hakemistoon ja ajaa skript ohjelma, joka lisää kutsun alkuun https: ja loppuun /owa. Kaikkia kutsumahdollisuuksia ei kuitenkaan saada tällä tavalla katetuiksi.

Toinen vaihtoehto on reitittää kaikki kutsut /owa –hakemistoon /owa hakemistoissa vaaditaan SSL-suojasta. Mikäli suojasta ei ole (<http://palvelin/owa>), niin kutsutaan virheenkäsittelijää 403;4, joka vuorostaan kutsuu html-tiedostoa, joka reitittää www-selaimen oikeaan paikkaan oikeilla parametreilla.

Konfigurointi suoritetaan seuraavasti

- SSL laitetaan päälle Default WebSiteen- ja sillä pitää olla varmenne
- Forms-autentikointi on käännetty päälle toisessa kohdassa Exchange CommandShell käskyllä
- Kaikkiin seuraavissa konfiguroinneissa tuleviin ”inheritance overridess” –kysymyksiin vastataan seuraavasti: ei valita mitään ja kuitataan ok.
- Web Sites-Default Web Sites ->OWA /Properties->Require SSL ( 128 –bit encryption)
- Web Sites-Default Web Sites ->Public /Properties->Require SSL ( 128 –bit encryption)
- :\\inetpub\\wwwroot ->ssldirect.htm-tiedosto
- Tiedoston sisältö (<servername> korvataan kyseisellä cas palvelimen nimellä ja selvitysteksti muokataan sopivaan ilmaisuun Vietnamiksi)
- Kun konfiguroidaa ntoista CAS2 palvelinta on tärkeää, että tiedosto tallennetaan c:\\inetpub\\wwwroot –hakemistoon paikallisen notepad ohjelman avulla (eikä kopioimalla sitä muualta)- eli tiedostoa ei saa editoida notepadilla CAS1 palvelimella ja sitten kopioida CAS2 palvelimelle

### **10.23 Exchange palvelinten paikalliset administrator ylläpitoryhmät**

Toimiakseen Exchange –palvelinten paikalliseen administrators ryhmän jäsenyyksien tulee olla kunnossa.

CAS- ja Hub-palvelinten paikallisessa administrator ryhmässä on kolme jäsentä

- Administrator (paikallinen)
- Toimialueen Domain Admin
- Toimialueen Exchange Organization Administrators

Ja Mailbox-palvelimen paikalliseen administrator ryhmään jäsenet

- Administrator (paikallinen)
- Domain Admins
- Toimialueen Exchange Organizations Administrators
- Toimialueen ClusterAdmin (toimialueessa user –tasoinen tunnus)

## 10.24 CCR -klusterin toiminnallisuuden testaaminen

Exchange 2007 –CCR klustereiden itse klusterointiin liittyvän toiminnallisuuden ylläpito tehdään Exchange Management Shell tai Exchange 2007 Management Console ohjelmalla. Perinteistä Cluster Administrator –ohjelmaa ei siis käytetä muuten kuin klusterin resurssien ja Cluster Group –perustoimintojen tilan tarkkailemiseen

Tähän kappaleeseen keräsin esimerkiksi muutamia PowerShell käskyjä, joilla voidaan tutkia ja hallita CCR-klustereita.

Seuraavalla käskyllä listataan CCR-klusteroidun sähköpostipalvelimen ominaisuuksia esim AutoDatabaseMountDial ja ForceDatabaseMountAfter

- get-mailboxServer <CMSName> | format-list (tai FL)

Seuraavalla käskyllä siirretään klusteroitu sähköpostipalvelu CCR klusteri toiseen noodiin

- Move-ClusteredMailboxServer –Identity >CMSName> -TargetMachine <nodename>

Mikäli klusteroidun sähköpostipalvelimen siirtäminen CCR-klusterin nodelta toiselle epäonnistuu ja sähköpostikanta vaurioituu, kantaa voidaan yrittää palauttaa seuraavalla käskyllä

- restore-StorageGroupCopy

Seuraavalla käskyllä voidaan listata nykyiset sähköpostipalvelimen käyttämän hub transport palvelimen ns ”current transport dumpster settings” asetukset

- get-TransportConfig | FL

CCR-klusterin tilan replikoinnin tilan voi tarkistaa seuraavalla käskyllä se kertoo CCR-klusterin tilanteen vaikka toinen node olisikin pois päältä

- get-ClusteredMailboxServerStatus <CMSName> | FL

CCR-Klusterin replikoinnin tilan voi tarkistaa seuraavalla käskyllä

- get-StorageGroupCopyStatus

Sähköpostipalvelimen tilan peruskäsky on

- get-ExchangeServer | Format-List

<http://technet.microsoft.com/en-us/library/bb124721.aspx> y

<http://www.microsoft.com/technet/prodtechnol/exchange/articles/e2k7/setupopten.msp> z

## 10.27 DTC konfiguraation avaaminen

Kun palvelimesta on tehty domain kontroller ja siihen on asennettu windows server 2003 sp 1 palvelin ei aina havaitse dcpromo- ohjelman ajamista ”promotea” riittävän hyvin DC palvelimen event lokiin tulee tällöin ilmoituksia asiasta.

## 10.28 SPAM filteröinti Sender-ID

Seuraavissa kappaleissa käsitellään sähköpostin lähettämistä internet DNS palveluiden avulla Sende-ID ja SPF tarkistavat molemmat sähköpostin lähettäjän viestin From kentästä. Kumpaakaan ei luonnollisesti kannata käyttää ainoana tekniikkana.

Tekniikat vertaavat lähettäjän tunnistetta viestin lähettäneeseen palvelimeen ja toisaalta DNS palvelun sisältämiin tietoihin. Sender Id tutkii viestin ns.MIME dataaja SPF etsii from kentän sisällön smtp protokollasta.

DNS erityisesti tähän käyttöön sovitettu TXT kenttä kertoo millä palvelimella on oikeus lähettää viestejä tietyn domainin nimissä. Jos palvelinta ei ole merkitty oikeuden haltijoiden listaan viesti tulkitaan roskapostiksi.

Mikäli DNS TXT tietuetta ei ole luovutettu domainille, niin SENDER ID tai SPD suodattimia ei käytetä ja roskapostin tunnistaminen jää muille SPÄM suodattimille. Myöskään kaikki DNS palveluita tarjoavat operaattorit eivät vielä tue DNS TXT tietueita.

Erityisesti Forwardoinnissa tulee kyseinen SPÄM torjuntatekniikka testata huolellisesti. FROM osoite kuitenkin säilyy samana sähköpostin koko kulkureitin ajan. Todennäköisesti forwardoivaa sähköpostipalvelinta ei ole auktorisoitu lähettämään sähköpostia FROM kentän mainitun viestin lähettäjän domainissa.

## 10.29 SPAM filteröinti SPF

SPF eli sender permitted from tai sender policy framework perustuu kuten Sender Id tekniikka siihen, että yritysten domainin on luotettujen sähköpostipalvelinten joukossa.

SPF kuten Sender Id luottaa tietoturvan parantamisessa internet DNS nimipalveluihin vaikkei DNS itse asiassa ole mikään turvapalvelu eikä sellaiseksi suunniteltu.

Onkin kyseenalaista voiko julkisen hallinnon (Quang Trin koulut) organisaatio tiukentaa

tietoturvaa Sender-Id:n avulla ja SPF esittämällä tavalla. Viranomaiset luultavasti joutuvat päästämään paljon sellaistaakin postia lävitse joka yksityisellä puolella estettäisiin.

Toisaalta mikä estää määrittelemästä Sender-Id:tä/SPF:ää, tällöin QTTC:n lähettäjän sähköpostia ei ainakaan tulkita roskapostiksi vain siksi, että Sender ID/SPF määritystä ei ole.

### **10.30 SPAM –filterointi: SIDF ja DKIM**

SIDF on yhdistelmä Sender-ID:tä ja SPF:ää SIDF tulee sanoista Sender ID Framework (RFC-4405-4408) ja DKIM sanoista Domainkeys identified mail (RFC-4871).

Ensin mainitussa varmennetaan lähettäjän postipalvelin ja jälkimmäisessä postipalvelin allekirjoittaa lähettämänsä viestit digitaalisesti (ja julkaisee varmenteensa DNS palvelussa).

Kaikkia näissä kappaleissa kerrottuja tekniikoita käytetään sähköpostin lähettäjän todentamiseen.



## 11. Exchange 2003->Exchange 2007 migraation vaiheet

Kaikkein tärkein huomioon otettava haastava asia on sähköpostien reitittäminen ennen migraatiota, migraatioiden aikana ja jälkeen

Alla olevassa listassa on koottuna Exchange 2003->Exchange 2007 –migraation pääkohdat.

### 11.1 Migraation kulku

Migraatio kannattaa aloittaa ns. ”satelliittitoimipisteistä” Exchange sähköposti infrastruktuurin keskipiste Qtttc päivitetään viimeisenä. Näin ei pääse syntymään ns. Island ongelmia. Island ongelmalla tarkoitetaan tilannetta, jossa Exchange 2003-järjestelmät eivät osaa viestiä keskenään, koska välissä on Exchange 2007 toimipiste. Eikä tarvittavia routinggroup konnektoreita ja muita määrittämiä ole tehty.

Stepit:

- Auktorisoinnin tarkastus kannattaa tehdä Exchange 2003 SMTP-domain (e)ille (kaikkien olisi syytä olla auktorisoituja)
- Otetaan pois päältä ns. link state toiminnallisuus
  - o Disable Link State Minor Version (Up/Down state) propagation
  - o HKEY\_LOCAL\_MACHINES\System\CurrentControlSet\Services\RESvc\Parameters
  - o Add Value: SuppressStateChanges tyyppi :REG\_DWORD. Value data: 1 (mikä muu kuin 0, niin estetään kaikki ”link state change” muutokset kyseisellä palvelimella (oletus on 0))
  - o Edellinen toimenpide tehdään jo ennen migraatiota
  - o Asennetaan ensimmäinen CAS-palvelin ”Central siteen” (Qtttc)
  - o Asennetaan ensimmäinen Hub palvelin ”central siteen”
    - Kytkeytyvätkö CAS ja Hub palvelimet Exchange 2003 postilaatikkopalvelimeen (palvelimiin) koskaan?
    - Luodaan routing group konektori ”central siteen” ja kaikkien Exchange

2003 ”satelliitti sitejen ” välille

- Link state kustannus 100?
- Asennetaan sähköpostilaatikkopalvelimet ”central siteen”
- Replikoidaan julkiset kansiot (public folders) Exchange 2007 ympäristöön työvälineenä on Exchange 2003 System Manager tai PFDaVAdmin (PFDaVAdmin on tehokas luvitusten määrittelemisessä)
- Aina kun poistetaan Exchange 2003 site niin luodaan routing group Konnektori ”ohi” poistetun siten. ”Link state cost” laitetaan arvoon 100 (ja käynnistetään palvelimet uudelleen)

## 11.2 Sähköpostilaatikoiden migrointi

Sähköpostilaatikat migroidaan eli siirretään Exchange 2003 ->Exchange 2007 Exchange Management Shellin move-mailbox –cmdlet käskyllä.

Mikäli move mailbox epäonnistuu esim. huonojen tietoliikenneyhteyksien takia, move mailbox voidaan suorittaa uudelleen ongelmitta. Uusinta toimenpide on ok sekä lähtöpään että kohdepään osalta.

## 11.3 Alustavat toimenpiteet

Tässä kappaleessa on joukko alustavia toimenpiteitä, joilla valmistellaan sähköpostilaatikoiden siirtämistä uuteen Exchange ympäristöön.

- Valmistellaan Active Directory Exchange 2007:n asentamista varten
  - o (setup/PrepareLegacyExchangePermissions, PrepareSchema, PrepareAd)
- Asennetaan Exchange 2007 palvelimet Exchange 2003 organisaatioon ja laitetaan Exchange 2007 käyttämään Exchange 2003 järjestelmää sähköpostin reitityksessä
- Viimeistellään konfiguraatio
  - o Luodaan mm. varmenteet (subject alternative name –määrittelyksellä, jolloin saadaan samaan CAS edustapalvelimeen Outlook Anywhere, Outlook Web Access, AutoDiscovery palvelu, ActiveSync jne)
- Luodaan Storage Group ja Mailbox Store sähköpostivarastot (tuhotaan oletuksena

syntyvä First Storage Group ja sen Mailbox Database)

#### 11.4 Sähköpostilaatikoiden ym. siirtäminen

Tässä kappaleessa kuvaan varsinaiset sähköpostilaatikoiden ja Exchange 2003 resurssien siirtäminen uuteen Exchange 2007 SP1 ympäristöön.

Siirretään ensimmäiset testipostilaatikot Exchange 2007 SP 1 ympäristöön.

- Siirretään ensimmäiset testipostilaatikot Exchange 2003 ympäristöstä Exchange 2007 ympäristöön käyttäen Exchange 2007 Management Shell ohjelmia
- Replikoidaan public folderit, system folderit Exchange 2007 ympäristöön
- Muutetaan ns. offline address book palvelin Exchange 2003:sta 2007:ään
- Siirretään public folder hierarkia Exchange 2003:sta Exchange 2007:ään
- Siirretään SMTP konnektori Exchange 2003:sta Exchange 2007:ään
  - o Käytännössä luodaan uusi SendConnector Exchange 2007:ään. Korvataan tällä uudella konnektorilla Exchange 2003:n SMTP konnektori
- Työasemien kytkeytyminen uuteen sähköpostipalvelimeen kestää aikansa. Onkin suositeltavaa että vanha sähköpostijärjestelmä pidetään päällä vielä ainakin kuukauden, jotta työasemat ehtivät kytkeytä uusiin palveluihin.

#### 11.5 Vanhan järjestelmän alasajo

Vanhan Exchange 2003 ympäristön alasajo kestää viikkoja jopa kuukausia. Tähän kappaleeseen olen kuvannut karkealla tasolla vanhan ympäristön alasajon toimenpiteet

- varmistetaan, että Exchange 2003:ssa ole enää public foldereita ja tuhoetaan public folder store
- Varmistetaan, että organisaatiossa ole enää Exchange 2003 sähköpostilaatikoita
- Tuhotaan Exchange 2003 mailbox storet
- Varmistetaan, että sähköpostit kulkevat Exchange 2007 ympäristössä ongelmitta
- Varmistetaan, että kaikki uudet ulkoiset sähköpostipalvelut (Outlook Anywhere, OWA, ActiveSync) toimivat ongelmitta
- Poistetaan konnektorit (SMTP connector to "internet" ja routing Group Connector Exchange2003 ->Exchange 2007 ja Exchange 2007->Exchange 2003
  - o Exchange 2007:n asennus on alunperin luonut edellämainitut routin group

konnktorit Exchange 2003 ja Exchange 2007 välille automaattisesti

- Muutetaan Exchange 2003 Recipient Policy Exchange 2007:n Email Address Policyksi (LDAP filter->OPATH)
- Tuhotaan vanha domain Recipient Update Service Exchange 2003 ohjelmalla paitsi Management Tools ylläpito välineet
- Tuhotaan First routing group objekti
- Huom. vanhoja Exchange 2003 administrative group objekstia ei saa tuhota (kun käytössä on outlook 2003 :free-busy tietoken käyttö voi estyä ja luvitusten delegointi vaarantua)
- Outlook 2003 työasemaohjelmat käyttävät system foldereita asetustensa tallentamiseen näin ollen myös system folderit on migroitava huolellisesti

## 11.6 Käsintehdyt SMTP osoitteet

Käsintehdyt SMTP osoitteiden kanssa on oltava tarkkana.

Käsintehdyt osoitteita on mm. resurssipostilaatikoilla, varmistettava, että exchange 2007 osoitin politiikat (address policy) eivät vahingossa pure näitä postilaatikoita.

## 11.7 Migraatiotunnukset

Migraatiota varten tulee käytössä olla joukko voimakkaita tunnuksia, joilla siirtäminen kopioinnit ja synkronoinnit tehdään. tunnuksilla tulee olla oikeudet sekä lähtö että kohdejärjestelmiin.

Tunnuksilla tulee luonnollisesti olla myös tarvittavat Exchange 2007 roolit ja oikeudet.

## 11.8 Palvelinten määrä

Tässä esitetään suositus palvelinten määrästä.

Kappaleessa mainittujen palvelinten lisäksi voidaan käyttää Hyper-V virtuaalikoneita. Yhden host palvelimen myötä saadaan varakäyttöä varten esimerkiksi yksi Hub-palvelin yksi CAS palvelin ja yksi 1+1 CCR klusteri

Vara virtuaalikoneita on syytä olla päällä jatkuvasti, jotteivät esimerkiksi niiden konetilien salasanat vanhene. Lisäksi kyseisessä host palvelimessa voi olla tulostus ja tiedostonjakopalvelimet toimialueen vara-hallinta kone (DC) Järjestelmänhallinnan palvelin jne.

On syytä huomata, että mitoitukseseen ei vaikuta se ovatko työasemat Outlook 2003 vai Outlook 2007 versioita. Työasema ohjelmia on ehdottomasti syytä käyttää ns. cached tilassa.

2 aktiivista 2 passiivista sähköpostipalvelinta CCR klusterissa

Tämä tarkoittaa 1500 käyttäjää per postipalvelin. (Tämä kuulostaa järeältä palvelimelta on esitetty ajatuksia siitä, että kouluun sulautetaan toisia kouluja, näin ollen käytön määrä tulee kasvamaan). Tehojen kannalta riittäisi hyvinkin yksi 1+1 CCR klusteri, mutta vikasietoisuuden ja korkean käytettävyyden postinkäsittely operaatioiden ym. vuoksi on hyvä olla varalla toinen klusteri

- Keskusmuistia mikäli mahdollista 32GB, jos ei onnistu niin hätätapauksessa 16GB riittää
- Kaikissa palvelimissa 1 4 ytiminen prosessori
- Tarvittava massamuistikapasiteetti on seuraavanlainen

Storage group count	Exchange 2007 minimum required physical memory	Exchange 2007 SP1 physical memory
1-4	2GB	2GB
5-8	4GB	4GB
9-12	6GB	5GB
13-16	8GB	6GB
17-20	10GB	7GB
21-24	12GB	8GB
25-28	14GB	9GB
29-32	16GB	10GB

Taulukko 1: Exchange 2007 vaatima muistilisäys tietokantojen lisääntyessä

2Hub transport palvelinta

- keskusmuistia 8GB (mikäli jostain halutaan säästää niin 4GB riittää). Tarkempaa tietoa kuormituksesta ei ole tällä hetkellä saatavissa.
- 1 4 ytimen prosessori /palvelin
- kaksi hub palvelinta riittää vaikka onkin otettu huomioon korkean käytettävyyden vaatimukset

## 2 Client Access palvelinta

- Keskusmuisti 8GB
- Yksi 4 ytimen prosessori
- kaksi CAS palvelinta riittää vaikka otetaan huomioon korkean käytettävyyden vaatimukset

Exchange sähköpostijärjestelmää on tarkoitus valvoa Microsoftin System Center Operations Manager 2007 Ohjelmalla tästä tulee kokoonpanoon 2 palvelinta lisäksi kummassakin on 1 kappale 4 ytimistä prosessoreita ja 4 GB keskusmuistia

Exchange 2007 tarvitsee tehokkaasti toimiakseen nopean yhteyden DC palvelimeen, johon määritelly Global Catalog palvelu. Näitä DC palvelimia on korkean käytettävyyden vuoksi salissa oltava vähintään kaksi. On tärkeää, että koko AD hakemisto mahtuu näiden DC/GC palvelinten keskusmuistiin. Tämän takaamiseksi voidaan käyttää 64 bittisiä käyttöjärjestelmiä.

## 12. Outlook 2003 profiilit

Koska kyse on Exchange organisaation sisäisestä migraatiosta niin outlook 2003 työasemien Outlook profiilit päivittyvät automaattisesti osoittamaan uusia sähköpostipalvelimia. Profiilien päivittyminen edellyttää, että vanha exchange 2003 palvelin on päällä ja toimii normaalisti.

Mikäli vanha Exchange 2003 palvelin on pois päältä, voidaan työasemia auttaa DNS määrittämisen avulla. Luodaan DNS:ään A host eli tietue, jonka nimenä on vanhan Exchange 2003 palvelimen nimi. Tämä host tietue laitetaan osoittamaan mihinkä tahansa vanhaan exchange 2003 palvelimeen. Itse asiassa kyseinen ”vanha” exchange palvelin voi olla jopa domain controller - palvelin, jossa on aktivoituna Global Catalog palvelu (kunhan palvelimessa on toimiva ns. NSPI eli Name Service Provider Interface-verkkoliitymä).

### 13. Tietoliikenteen määrät

Tietoliikenteen määriä arvioitaessa joudutaan tekemään suuri joukko oletuksia.

Sähköpostijärjestelmän tarvitsema tietoliikenneyhteyksien nopeus määrittyy mm seuraavien tekijöiden perusteella. Oletukset on tehty tietoliikenteen määrälle, saadaan realistinen lähtöarvio.

- Tärkein kysymys: mitä muuta menee Exchange yhteyksien kautta kuin itse sähköpostiliikennettä? Ulkoista liikennettä, sisäistä liikennettä?
- Tietoliikenteen määrä ei johdu sähköpostilaatikon koosta
- Kirjautumiset login (normaali Outlook kerran Owa 2 kertaa päivässä)
- Klientin tyyppi Outlook 2003 vai Outlook 2007
- Cached vs online mode (cached ja Outlook anywhere toimivat paikallista kantaa vasten)
- Profiili kevyt/normaali/raska/erittäin raskas
- Lukemiset, tuhoamiset lähettämiset
- Huiput 2-3 kertaa normaalikuormitus
- Aktiivinen aika (tunteina vuorokaudessa)
- Luetaanko kaikki saapuneet viestit
- puolet tulleista viesteistä tuhotaan
- miten hakemistoja käytetään
- viestin koko esim 50kb



## 14. Sähköpostijärjestelmän mahdollisesti kokemat nykyiset/tulevat haasteet

Oman haasteensa ympäristöön tuo Vietnamin ilmasto. Vuodenaikoja ei ole kuin kuivakausi ja sadekaus, joten on ihan selvää että ongelmia esiintyy.

Lämpötila on välillä 21 -39C ja ilman kosteus 78-98% jatkuvasti. Varsinaisia konesaleja ei ole, joten palvelinten jäähydytyksessä on suuria ongelmia. Myöskään palvelintilat eivät ole likasuojattuja koska rakennuksissa ei ole ikkunalaseja.

Talkkimainen punainen pöly leviää kaikkialle tuulen mukana. Koska Vietnam on edelleen voimakkaasti kehittyvä maa, heillä ei ole käytössä vielä samaa tietotaitoa kuin esim. meillä Suomessa suojata laitteita.

Sähkön syöttö aiheuttaa myös ongelmia. Kun sähköstä on pulaa, saatetaan sähkökatkoksia aiheuttaa ihan sähkölaitoksen toimesta ennalta määrätyille alueille.

Tästä syystä mielestäni tarvitaan esim. dieselkäyttöinen aggregaatti syöttämään varavoimaa palvelimille katkoksen sattuessa.

Kuitenkin suurimman haasteen antaa tälle projektille paikallisten asiantuntijoiden ja koulujen johdon asenteet. Paikallisilla ylläpitäjillä on taipumusta kokeilla erilaisia asetuksia ilman suunnitelmaa/muistiinpanoja tehdyistä muutoksista tai alkuperäisistä asetuksista. Harvinaista ei ole myöskään toisten sähköpostien lukeminen ilman lupaa.

Esim. jos rehtori uskoo että häneltä pimitetään tietoja (vaikka kyseinen tieto ei hänelle kuulu), hän pyytää ylläpitäjältä pääsyn kyseisen henkilön sähköpostiin ja lukee viestit läpi. Vietnamsissa edelleen on vallalla ”isoveli valvoo asenne” ja kommunistisella puolueella on vahva asema.

Tietoturvatason olisi syytä nousta ja asenteiden muuttua. Eli vaikka luonto ja olosuhteet ovatkin rankat ja aiheuttavat monenlaisia ongelmia järjestelmälle, on kuitenkin koulun henkilökunta IT -järjestelmän pahin vihollinen.

## 15. Pohdinta

Työn tavoitteena on ollut tutustuttaa siihen työmäärään, joka tulee tehdä ennen kuin voidaan migraatio aloittaa. Yliheiton suunnittelu ja rakentaminen on aikaa vievää puuhaa, arviolta kaksi viikkoa olisi syytä varata näihin toimiin.

Opinnäytetyöni ohjeilla pystyin pystyttämään testiympäristön. Tämän opinnäytetyön avulla pystytään asentamaan ja yliheittämään Exchange 2003 Exchange 2007 ympäristöön myös isommassa mittakaavassa.

Kaikki käytössä olevat Exchange 2003 ympäristöt ovat lähtökohtaisesti samanlaisin mutta jokaisessa yliheitossa esiintyvät ongelmat ovat erilaisia johtuen Exchange 2003 tehdyistä käyttäjäkohtaisista asetuksista ja mahdollisesta korruptoituneesta tiedosta jota yleensä esiintyy kun postilaatikkojen koko kasvaa liian suureksi. Kaikkea tällaista tietoa ei ole voitu ottaa tässä työssä huomioon vaan ne täytyy selvittää tapauskohtaisesti.

Olen itse koonnut testilaboratorion Exchange 2003 ja 2007 ympäristöille. Olen saanut apua niin Windows palvelinasiantuntijoilta, verkkoasiantuntijoilta ja palvelinten kasaus asiantuntijoilta. Suuri kiitos heille!

Yleensä tämänkaltaiset projektit tehdään yhteistyössä eri ammattilaisten kesken. Kukaan ei tee tuotantoympäristössä yksin kaikkea. Koin haasteelliseksi sen, että työn toteuttaminen testiympäristössäkin vaati paljon eri alojen syvempää tietämystä. Työ onnistui mielestäni hyvin. Vaikka kyseessä ei ollutkaan oikea toimeksianto, on tätä opinnäytetyötä tehty kuin kyseessä olisi osa oikeata transitio projektia. Tavoite saavutettiin rakentamalla testilaboratorioon ympäristö joka pystytettiin kohta kohdalta perustuen tähän opinnäytetyöhön.

Matkan varrella on ollut haasteita ja ongelmia oli matkan varrella. Oma asiantuntijuus oli merkittävässä asemassa, koska työssäni olen ollut nimenomaan sähköpostiasiantuntija. Mielestäni työssä hankitusta asiantuntijuudesta, on ollut varsin paljon apua tätä opinnäytetyötä tehdessä.

Jatkotutkimuksena voisi ottaa vaikka koulun AD rakenteen tarkasteluun. Tutkimus on myös hyvä pohja uusien exchange migraatioiden tekemiseen tulevaisuudessa. Tutkimus on mielestäni luotettava ja eettisesti hyvä. On otettava huomioon, että tietyt asiat tehdään Vietnamsissa eri lailla. Kun muistaa sen, että eri kulttuureissa on erilainen tapa työskennellä. Tuloksena tämä

opinnäytetyö sai aikaan onnistuneen migraation ainakin testiympäristössä.

## 16. Lähteet

Barry Gerber, Jim McBee 2008: Mastering Exchange Server 2007 | ISBN-10: 0470042893 | ISBN-13: 978-0470042892 | Edition: 1

David W. Tschanz 2008: Exchange Server 2007 Infrastructure Design: A Self Orient Approach ISBN: 978-0-4702-2446-5

Jim McBee, Benjamin Graig 2008: Exchange Server 2007 Implementation & Administration ISBN: 978-0-470-1874-8

Microsoft Official Course 3938B: Updating Your Skills From Microsoft Exchange 2000 Server or Microsoft Exchange 2003 to Microsoft Exchange Server 2007 Microsoft course Course 3938C

Rawlinson Rivera 2008: MCITP: Microsoft Exchange Server 2007 Messaging, Design And Deployment Study Guide (Exams 70-237 & 70-238)

Will Schmied, Kevin Miller 2008: MCTS: Microsoft Exchange Server 2007 Configuration Study Guide (Exam 70-236)

Paul Cunningham Exchange 2007 Transition Guide by Luettavissa:  
<http://exchangeserverpro.com/exchange-2007-transition-guide/> Luettu 1.8.2013

Transition from Exchange 2000/2003 to Exchange server 2007 by Henrik Walther [Published on 16 Jan. 2007 / Last Updated on 16 Jan. 2007]

Luettavissa: <http://www.msexchange.org/articles-tutorials/exchange-server-2007/migration-deployment/Transitioning-Exchange-2000-2003-Exchange-Server-2007-Part1.html> Luettu :1.8.2013.

Dan Holme, Nelson Ruest; Danielle Ruest: Configuring Windows Server 2008 Active Directory Microsoft press 2008 ISBN-13 978-0-7356-2508-2 ISBN-10 0-7356-2508-5

Mohammed Basher MFST 4.6.2008 [TechNet Blogs](#) > [Infrastructure snapshots](#) > [Exchange 2000/2003 to Exchange 2007 migration guidelines](#)  
Luettavissa: <http://blogs.technet.com/b/mbaher/archive/2008/06/04/migrating-exchange-2000-2003-to-exchange-2007-guidelines.aspx> Luettu :1.8.2013.

Siddarth Saijan 14.4 2012 Migrate Microsoft Exchange Server 2003 to 2007

Luettavissa: <http://siddarthsajjantechnotes.blogspot.fi/2012/04/migrate-microsoft-exchange-server-2003.html> Luettu : 9.8.2013

MarcGrote How the exchange server 2007 core services work together 24.7.2007 Luettavissa:

<http://www.msexchange.org/articles-tutorials/exchange-server-2007/planning-architecture/how-exchange-server-2007-core-services-work-together.html> Luettu : 4.5.2013

Marc Grote Exchange internals-How the exchange core components work together 15.6. 2006

Luettavissa: <http://www.msexchange.org/articles-tutorials/exchange-server-2003/planning-architecture/Exchange-Internals-How-Exchange-Core-Components-work-together.html> Luettu: 4.5.2013

## Liitteet

<http://www.microsoft.com/downloads/details.aspx?familyid0cb42fc06-50c7-47ed-a65c-862661742764&displaylang=eng> a

<http://www.microsoft.com/windowsserver2003/technologies/management/powershell/download.d.aspx> b

(<http://www.microsoft.com/downloads/details.aspx?FamilyID=993C0BCF-3BCF-4009-BE21-27E85E1857B1&displaylang=en> c

<http://msexchange.com/archive/2008/11/21/450151.aspx> d

<http://technet.microsoft.com/en-us/library/bb125224.aspx> e

<http://support.microsoft.com/kb/157025> f

<http://support.microsoft.com/kb/894435> g

<http://go.microsoft.com/fwlink/?linkid=74465>. h

<http://support.microsoft.com/kb/894435> i

<http://support.microsoft.com/kb/894435> j

[http://technet.microsoft.com/en-us/library/bb232021\(EXCHG.80\).aspx](http://technet.microsoft.com/en-us/library/bb232021(EXCHG.80).aspx) k

<http://technet.microsoft.com> l

[http://technet.microsoft.com/en-us/library/bb738161\(EXCG.80\).aspx](http://technet.microsoft.com/en-us/library/bb738161(EXCG.80).aspx) m

[http://technet.microsoft.com/en-us/library/bb232021\(EXCG.80\).aspx](http://technet.microsoft.com/en-us/library/bb232021(EXCG.80).aspx) n

[http://technet.microsoft.com/en-us/library/aa998836\(EXCG.80\).aspx](http://technet.microsoft.com/en-us/library/aa998836(EXCG.80).aspx) o

[http://technet.microsoft.com/en-us/library/aa998294\(EXCG.80\).aspx](http://technet.microsoft.com/en-us/library/aa998294(EXCG.80).aspx) p

<http://www.microsoft.com/windowsserver2003/adam/default.aspx> q

<http://go.microsoft.com/?fwlinkid/=74465> r

<http://support.microsoft.com/kb/907265> s

(<http://www.microsoft.com/windowsserver2003/technologies/management/powershell/download.d.aspx> t

<http://support.microsoft.com/?kbid=921181> u

(<http://www.microsoft.com/downloads/details.aspx?FamilyID0aa353712-05e7-4b08-888c-f8ecb998dc72&DisplayLang=en> w

<http://go.microsoft.com/fwlink/?linkid=74465> x

<http://support.microsoft.com/kb/323431> y

[http://technet.microsoft.com/en-us/library/aa998327\(EXCHG.80\).aspx](http://technet.microsoft.com/en-us/library/aa998327(EXCHG.80).aspx) z

<http://technet.microsoft.com/en-us/library/bb124721.aspx> ä

<http://www.microsoft.com/technet/prodtechnol/exchange/articles/e2k7/setupten.msp>

<http://www.msexchange.org/articles-tutorials/exchange-server-2007/planning-architecture/how-exchange-server-2007-core-services-work-together.html> ä

<http://www.msexchange.org/articles-tutorials/exchange-server-2003/planning-architecture/Exchange-Internals-How-Exchange-Core-Components-work-together.html> ö