

PALVELIN KOTIIN

Windows Home Server & Amahi Home Server -kotipalvelinkäyttöjärjestelmät

Heikki Polo
Antti Seppänen
Opinnäytetyö
Syksy 2010
Tietojenkäsittely
Oulun seudun ammattikorkeakoulu

TIIVISTELMÄ

Oulun seudun ammattikorkeakoulu
Tietojenkäsittely

Tekijä(t): Heikki Polo, Antti Seppänen

Opinnäytetyön nimi: Palvelin kotiin – Windows Home Server & Amahi Home Server -
kotipalvelinkäyttöjärjestelmät

Työn ohjaaja(t): Eero Leskinen

Työn valmistumislukukausi ja -vuosi: Syksy 2010

Sivumäärä: 70

TIIVISTELMÄ

Saimme koulultamme opinnäytetyöaiheen ”Windows Home Server”. Myöhemmin aihe kuitenkin laajeni, eikä koskenut pelkästään enää Windows Home Serveriä, vaan myös Amahi Home Serveriä, jolloin saimme aiheeseemme enemmän syvyyttä ja mielenkiintoa.

Työssämme testataan kotiympäristössä yllämainittuja kotipalvelinkäyttöjärjestelmiä. Asennamme ja konfiguroimme ne, jonka jälkeen pohdimme ja kerromme omat mielipiteemme näiden ominaisuuksista, asennuksen ja käytön helppoudesta sekä toiminnallisuudesta, jotka ovat työn tuloksia. Työn tavoitteena on lähinnä tutustuttaa lukija kotipalvelinkäyttöjärjestelmiin, sekä antaa mielipiteitä kirjoittajien omista käyttökokemuksista molemmista järjestelmistä.

Työssä on käytetty alan kirjallisuutta koskien Windows Home Serveriä. Myös muutamia Internet-lähteitä on käytetty tietoperustan tukemiseen. Amahi Home Serveriin ei kirjallisuutta ole, joten siihen liittyvät lähteet ovat pelkästään Internetistä.

Työ sisältää tarkat ja vaiheistetut ohjeet molempien järjestelmien asentamisesta ja käyttöönottamisesta. Lisäksi työssä esitetään vertailua tiedonsiirtonopeuksista ja muutamia esimerkkejä tietoturvaan liittyvistä asioista ja tuloksista. Lukijan oletetaan osaavan tietotekniikan perusasioita, kuten verkkoihin ja lähiverkkoihin liittyvää osaamista, kokemusta käyttöjärjestelmien asentamisesta, tuntemusta tietokonelaitteistosta ja alan termistöstä.

Asiasanat: *Amahi Home Server, kotipalvelin, Nessus, palvelin, palvelinkäyttöjärjestelmä, Windows Home Server*

ABSTRACT

Oulu University of Applied Sciences
Degree Programme in Business Information Systems

Author(s): Heikki Polo, Antti Seppänen

Title of thesis: Server at home – Windows Home Server & Amahi Home Server operating systems

Supervisor(s): Eero Leskinen

Term and year when the thesis was submitted: Autumn 2010

Number of pages: 70

ABSTRACT

The topic of this thesis was initially Windows Home Server. Later on, the subject was expanded to include Amahi Home Server in addition to Windows Home Server. This added more depth and interest to this work.

The objective of this thesis is mainly to acquaint the reader with the two home server operating systems and to evaluate them based on empirical testing. The systems were tested and configured after which the properties of the systems were discussed and compared. The focus was on the easiness and functionality of installation and usage.

In the thesis, the theoretical background consists of literature on Windows Home Server. In addition, a few Internet sources have been used to support the background. There is no literature on Amahi Home Server and, therefore, the sources related to it are entirely from the Internet.

This thesis contains exact and phased instructions of the installation and configuration of both systems. Furthermore, a comparison of the data transfer rates, and a few data security related examples of the matters and results are presented in the thesis. A reader is expected to know the basics of the information technology which is related to the networks and to the local area networks. Moreover, he is expected to have experience of installing operating systems, knowledge of computer hardware and IT-related terminology.

Keywords: *Amahi Home Server, home server, Nessus, server, server operating system, Windows Home Server*

SISÄLTÖ

1	JOHDANTO	6
2	PALVELIN.....	7
3	KOTIPALVELIN	8
3.1	Windows Home Server	10
3.1.1	Ominaisuudet.....	10
3.1.2	Lisäominaisuudet (Add-ins)	11
3.1.3	Järjestelmävaatimukset	12
3.2	Amahi Home Server	13
3.2.1	Ominaisuudet.....	13
3.2.2	Lisäominaisuudet (Apps)	14
3.2.3	Järjestelmävaatimukset	14
4	TESTAUSSUUNNITELMA.....	16
5	KOTIPALVELINKÄYTTÖJÄRJESTELMIEN ASENNUS	18
5.1	Windows Home Server	18
5.2	Amahi Home Server	21
6	KÄYTTÖÖNOTTO JA KONFIGUROINTI.....	25
6.1	Windows Home Server	25
6.1.1	Kotitietokoneen liittäminen palvelimeen (Windows Home Server Connector)	25
6.1.2	Varmuuskopioiden hallinta (Computers & Backup).....	27
6.1.3	Käyttäjän lisääminen (User Accounts)	28
6.1.4	Jakokansiot (Shared Folders)	31
6.1.5	Verkon monitorointi (Network Healthy)	33
6.1.6	Palvelimen järjestelmäasetukset (Settings)	34
6.1.7	Etäyhteyden määrittely (Remote Access)	36
6.1.8	Etäyhteyden käyttäminen (HTTP Remote Access).....	38
6.1.9	Palvelimen turvallisuus	39
6.1.10	Median streamaus (Media Streaming/Media Sharing)	39
6.2	Amahi Home Server	41

6.2.1	Käyttäjien luominen (Users).....	42
6.2.2	Jakokansioiden luominen (Shares).....	42
6.2.3	Jakokansioiden muokkaaminen (Shares)	43
6.2.4	Jakokansioiden käyttäminen.....	44
6.2.5	Ohjelmien asentaminen (Apps).....	45
6.2.6	Osiot ja levyt (Storage)	46
6.2.7	Verkkohallinta (Networking)	47
6.2.8	Asetukset (Settings).....	47
6.2.9	Palvelimen lokitiedot (Debug)	48
6.2.10	Hakutoiminto (Search HDA/Web)	49
6.2.11	Varmuuskopioiden tekeminen.....	50
6.2.12	Streamaus Amahissa.....	51
6.3	Reitittimen konfigurointi	51
7	TIEDONSIIRTONOPEUDET.....	53
8	TIETOTURVATESTIT	56
9	KÄYTTÖKOKEMUKSET JÄRJESTELMISTÄ	64
9.1	Haitat	64
9.2	Edut	66
9.3	Yhteenveto	67
10	POHDINTA	68
	LÄHTEET	70

1 JOHDANTO

Nykyaikana monessa kodissa on paljon digitaalisia laitteita, kuten esimerkiksi tietokoneita, älypuhelimia, pelikonsoleja, digitaalikameroita ja MP3-soittimia. Näistä laitteista voi syntyä suuria määriä dataa, kuten kuvia, videoita, musiikkia ja muita tiedostoja, joita pitäisi pystyä hallitsemaan helposti. Viime vuosien saatossa on kehitetty kaksi kotipalvelinkäyttöjärjestelmää, jotka tarjoavat kotikäyttöön tarkoitettuja ratkaisuja laitteiden sekä datan hallitsemiseen ja ylläpitämiseen kotiverkossa.

Työssämme testataan kahta erilaista kotipalvelinkäyttöjärjestelmää Windows Home Serveriä ja Amahi Home Serveriä. Asennamme ja konfiguroimme ne, jonka jälkeen pohdimme ja kerromme mielipiteemme näiden ominaisuuksista, asennuksen ja käytön helppoudesta sekä toiminnallisuudesta.

Opinnäytetyön alussa kerrotaan yleisiä asioita palvelimesta, josta kerrotaan lukijalle tärkeimmät seikat, kuten mitä palvelimella tarkoitetaan ja mitä se tekee. Tämän jälkeen paneudutaan aiheeseen, jossa käsitellään kotipalvelinta ja sen käyttötarkoituksia. Lisäksi käymme läpi molemmista kotipalvelinkäyttöjärjestelmistä niiden ominaisuudet, järjestelmävaatimukset ja muut yleiset asiat.

Testaussuunnitelmakappaleessa perehdytään testauksen tavoitteisiin, testauskohteisiin, testausympäristöön, vertailukriteereihin, laitteistoihin sekä ohjelmistoihin. Testaussuunnitelman jälkeen työssämme kerrotaan ja ohjeistetaan miten molemmat järjestelmät asennetaan ja miten ne konfiguroidaan toimintakuntoon.

Esittelemme myös tuloksia järjestelmien tiedonsiirtonopeuksista ja tietoturvallisuustesteistä. Lopuksi kerromme omakohtaisia kokemuksia molemmista kotipalvelinkäyttöjärjestelmistä, ja annamme myös pohdintakappaleessa oman mielipiteemme ja perustelumme, kumpi näistä on parempi ottaa käyttöön kotiin, sekä omia tuntemuksia ja ajatuksia kyseisen opinnäytetyön tekemisestä.

2 PALVELIN

Palvelimella tarkoitetaan yleensä muun muassa web-palvelimia, tulostinpalvelimia, välityspalvelimia, varmuuskopointipalvelimia ja tiedostopalvelimia. Nämä ovat tietokonejärjestelmiä ja ohjelmia, jotka tuottavat palveluita toisten käytettäväksi. Palvelimet ovat yleensä erillään tavallisista tietokoneista, joita ihminen saattaa nähdä päivittäin esimerkiksi toimistoissa. Ne sijaitsevat muiden palvelimien kanssa jossakin palvelinhuoneessa, joita ylläpitää siihen tarkoitukseen koulutettu henkilö. (Kettell 2008, 3).

Palvelimen tarkoitus on tarjota käyttäjille palveluita tai ohjelmia verkon yli joko yrityksen sisäverkossa, paikallisesti, laajaverkon alueella tai Internet-yhteyden avulla. Tietokoneita, jotka ovat yhteydessä palvelimeen ja käyttävät sen palveluita, kutsutaan asiakkiksi eli asiakaskoneiksi. (Kettell 2008, 3-4).

Palvelimen keskeisin tarkoitus on hallita isoja kokonaisuuksia, eli toisin sanoen suuria määriä samanaikaisia käyttäjiä ja heidän ajamiaan palveluita, jolloin palvelimen resurssit, kuten esimerkiksi prosessorin, tulee olla tehokas ja muistin määrä ja tallennuskapasiteetti suuria, jotta palvelin pystyy käsittelemään massiivisia määriä dataa jouhevasti.

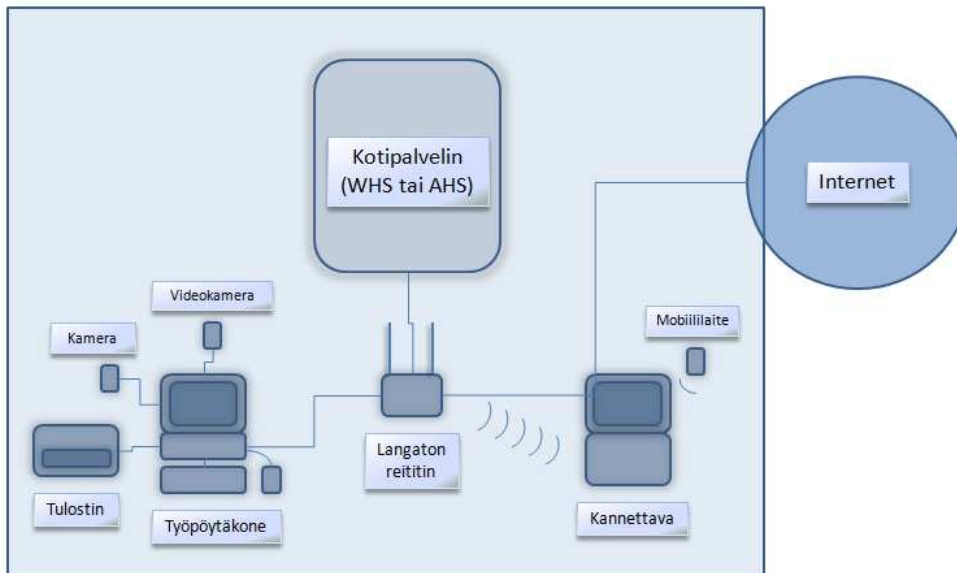
Kuten tavallisissa tietokoneissa, myös palvelimissa on käyttöjärjestelmä, joka pääasiassa eroaa tavallisesta käyttöjärjestelmästä lähinnä käyttöliittymältään, ominaisuuksiltaan ja toimivuudeltaan. Siinä missä tavallinen käyttöjärjestelmä tarjoaa rikkaan ja helppokäyttöisen käyttöliittymän, graafisia hienouksia ja työpöytäsovelluksia, pyrkii palvelinkäyttöjärjestelmä keskittymään lähinnä tehokkuuteen, varastointiin ja työkaluihin, jotka helpottavat palvelinohjelmistojen ajamista. Tyypillisiä palvelinkäyttöjärjestelmiä ovat Windows Server 2003 ja 2008, Linux sekä Unix. (Kettell, 2008, 3).

3 KOTIPALVELIN

Palvelimet ovat alkaneet siirtymään hiljalleen myös kotikäyttöön. Ne tarjoavat hyödyllisiä palveluita kotiverkkoihin, kuten esimerkiksi kaikkien kotikoneiden automaattisen varmuuskopioinnin, keskitetyn ja suojatun paikan kotikäyttäjien tiedostoille ja muita hyödyllisiä ominaisuuksia, kuten esimerkiksi media streaming-palvelun kotiverkon laitteille. Streaming, eli toisin sanoen suoratoisto, mahdollistaa videon tai äänen toistamisen sitä mukaan kun sitä ladataan.

Kotipalvelinkäyttäjärjestelmissä, kuten Windows Home Serverissä ja Amahi Home Serverissä yhdistyvät ikään kuin sekä tavallisen käyttöjärjestelmän että palvelinkäyttäjärjestelmän toiminnot tavalla, joka mahdollistaa yksinkertaisen ja helposti hallittavan järjestelmän käyttäjille. Kotipalvelinkäyttäjärjestelmän idea, käyttökohteet ja palvelut ovat siis hiukan riisutummalla ja yksinkertaisemmalla verrattuna normaaliin palvelinkäyttäjärjestelmään, sillä esimerkiksi Windows Home Serveristä ei löydy mitään AD:n (Active Directory) kaltaisia palvelinrooleja, ryhmäkäytäntöjä (Group Policy) tai muita edistyksellisempiä ominaisuuksia.

Nykyään monessa kodissa tai perheessä on usein enemmän kuin yksi tietokone. Lisäksi monella on pelikonsolit, tulostimet, älypuhelimet ja mahdollisesti myös muita verkkoon kytkettyjä laitteita. Näiden laitteiden välinen tiedostojen jakaminen voi olla hankalaa, varsinkin jos niissä on eri käyttöjärjestelmät tai tietoturvaohjelmistot. Voi syntyä hankalia tilanteita, jossa esimerkiksi tiedostonjako tai tulostin on kytketty tiettyyn koneeseen, joka ei olekaan päällä tai kytkettynä verkkoon. Lisäksi harva ihminen huolehtii säännöllisistä varmuuskopioinneista. Tämän kaaoksen keskelle olisi järkevää asentaa kotipalvelinjärjestelmä, jota kaikki nämä laitteet voisivat keskenään hyödyntää. (Kuvio 1). (Kettel 2008, 5).



KUVIO 1. Kotipalvelinjärjestelmä ja kotiverkko

Kotipalvelinjärjestelmä on ns. piilossa oleva tietokone ilman oheislaitteita, eli näyttöä, näppäimistöä ja hiirtä. On kuitenkin huomioitava, että kyseisiä oheislaitteita tarvitaan järjestelmän asennuksen ja konfiguroinnin aikana. Näiden toimintojen jälkeen järjestelmää hallitaan kotiverkkoon liitetyllä koneella tai etäyhteyden avulla. (Hallihan 2008, 1.)

Kotipalvelinjärjestelmän tarkoituksena on tuoda kotiin ohjelmisto ja laitteistopaketti, jota on helppo hallinnoida ja jolla voidaan käyttää sekä suojata kotiverkkoja. Keskeisimpiä kotipalvelinjärjestelmän tehtäviä ovat automaattinen varmuuskopiointi, keskitetty tiedostonjako, yksinkertainen verkkohallinta, kotitietokoneiden suojaus, median streamaus sekä järjestelmän etähallinta joko lähiverkon tai Internetin kautta. (McFedries 2008, 9.)

Kotipalvelinjärjestelmä koostuu siis palvelinkoneesta sekä ohjelmistosta, eli käyttöjärjestelmästä. Saatavilla olevia ohjelmistoja ovat ainakin tällä hetkellä Windows Home Server sekä Amahi Home Server – kotipalvelinkäyttöjärjestelmät. Näistä kerromme tarkemmin seuraavissa luvuissa.

3.1 Windows Home Server

Windows Home Server pohjautuu Microsoftin aiempaan Windows Server 2003 - palvelinkäyttöjärjestelmään. Windows Home Serverin käytettävyys ja hallittavuus on muutettu kuitenkin melko erilaiseksi, sillä sitä hallinnoidaan pääasiassa Windows Home Server Consolella, joka on käyttäjäystävällinen, selkeä ja helppokäyttöinen. (McFedries 2008, 9.) Halutessaan Windows Home Serveriä voidaan käyttää työpöydältäkin, jolloin se muistuttaa käytettävyydeltään Windows Server 2003 –käyttöjärjestelmää.

Windows Home Serveriä ryhdyttiin kehittämään vuonna 2004 koodinimellä Q tai Quattro. Koodinimestä tuli siis viimein Windows Home Server ja siitä julkistettiin beta-versio aikaisin vuonna 2007. Yli 60 000 ihmistä kokeili Windows Home Serveriä maailmanlaajuisesti. (Edney 2007, 1.)

Microsoft myy Windows Home Servereitä pääasiassa valmiina konepaketteina. Käyttäjän ei tarvitse periaatteessa kuin kytkeä palvelin ja kotiverkon tietokoneet toisiinsa ja tehdä tarvittavat asetukset Windows Home Server Consoleen. On kuitenkin mahdollista valjastaa esimerkiksi vanha kotitietokone kotipalvelinkäyttöön ja ostaa pelkkä Windows Home Server –käyttöjärjestelmä, joka on huomattavasti halvempi vaihtoehto. Tässä opinnäytetyössä toteutamme jälkimmäisen vaihtoehdon asentamalla Windows Home Serverin ja verrokkijärjestelmän vanhaan kotitietokoneeseen.

3.1.1 Ominaisuudet

WHS:ssä on paljon hyödyllisiä ominaisuuksia, joista on hyvä mainita muutama. Se sisältää esimerkiksi automaattisen varmuuskopioinnin, jokaiselle asiakaskoneelle, jolle luodaan oma aikataulu. Varmuuskopioidut tiedostot voidaan palauttaa helposti muutamalla hiiren klikkauksella.

Tiedostoja, kuten musiikkia, videoita ja kuvia voidaan jakaa laittamalla ne jakokansioon ja varmistamalla, että muilla käyttäjillä on kansioon käyttöoikeudet. Tietokoneisiin ja tiedostoihin on mahdollista päästä käsiksi

mistäpäin maailmaa tahansa kirjautumalla Windows Live -palveluun, joka yhdistää käyttäjän Windows Home Serveriin. Kaikkiin jaettuihin tiedostoihin pääsee käsiksi yhdestä paikasta, sillä levykirjainten sijaan näkyy vain jaetut kansiot.

Kovalevytilaa voi laajentaa Windows Home Server Drive Extenderillä, joka mahdollistaa kovalevyjen lisäämisen helposti sekä sisäisesti että ulkoisesti. Jos haluaa varmistaa, että jaettavat tiedostot ovat saatavilla, vaikka yksi kovalevy lakkaisi toimimasta, voi kansioita monistaa useammalle kovalevylle muutamalla hiiren klikkauksella.

Vian sattuessa tietokoneen voi palauttaa toimintakuntoon Windows Home Server – palautuslevyllä. Windows Home Server Consolen avulla voi tarkastaa kaikkien verkkoon liitettyjen tietokoneiden tilan yhdestä paikasta.

Lisäksi WHS:ssä on yksinkertainen ja helppo käyttäjien lisääminen ja poisto sekä oikeuksien muokkaaminen. WHS:ään voi yhdistää maksimissaan 10 kotitietokonetta. Mediaa kuten kuvia, videoita ja musiikkia voidaan jakaa muille lähiverkossa oleville laitteille, jotka tukevat Windows Media Connectia, kuten esim. Xbox 360. (Edney 2007, 2-3.)

3.1.2 Lisäominaisuudet (Add-ins)

Windows Home Serverin toiminallisuutta voidaan laajentaa erikseen Internetistä ladattavilla lisäominaisuuksilla, eli Add-ineillä. Konsolinäkymässä ei ole oletuksena muuta kuin lähinnä perusominaisuuksia, joilla palvelimen toimintaa hallitaan. Add-ineillä voidaan lisätä konsoliin monenlaisia lisäominaisuuksia, kuten esimerkiksi etävalvontatyökaluja, kehittyneemmän konsolinäkymän, virustorjuntaohjelmistoja, levynhallintatyökaluja ja monia muita. (Most Popular Windows Home Server Add-ins, hakupäivä 18.6.2010).

Parhaimman paikan lisäominaisuuksien asentamiseen tarjoaa <http://www.wegotsserved.com> –sivusto, josta löytyy mittava kokoelma erilaisia Add-inejä moneen tarkoitukseen, kuten esimerkiksi turvallisuuteen, hallittavuuteen, varmuuskopiointiin, etäyhteyksiin ja ylläpitoon. Muutamia

mainittavia hyödyllisiä Add-inejä ovat muun muassa P80, joka luo WHS:ään web-sivuston, joka tarjoaa hyödyllistä nippelitietoa palvelimesta, Advanced Admin Console, jolla pääsee käsiksi WHS:n työpöydälle ja hallintapaikkoihin etäyhteydellä sekä näppärä ja hyödyllinen WHS Widget –ohjelma, jolla voi laittaa palvelimen kirjautumissivulle päivää piristävän widgetin, jossa voi pyöriä esimerkiksi vanha kunnan Pong tai Duck Hunt.

3.1.3 Järjestelmävaatimukset

Windows Home Serverin järjestelmävaatimukset eivät ole nykymittapuun mukaan kovin vaativia, kuten taulukosta (Kuvio 2) näkyy. Monesta muutamia vuosia vanhasta tietokoneesta voi valjastaa palvelimen Windows Home Serveriä varten.

KUVIO 2. Windows Home Serverin järjestelmävaatimukset

Vaatimukset	Minimi	Suositus
Prosessori	1 GHz Pentium 3 (tai vastaava)	Pentium 4, AMD x64 tai uudempi prosessori
Muisti	512 MB	512 MB
Kovalevytila	70 GB sisäinen kovalevy (ATA, SATA tai SCSI) ensisijaisena	Vähintään. kaksi sisäistä kovalevyä yht. 300 GB ensisijaisena
Verkko	100 Mbps verkkokortti	100 Mbps (tai nopeampi) verkkokortti

Microsoft on ilmoittanut, että tulevat versiot saattavat tukea ainoastaan 64-bittisiä prosessoreita. Olisi suositeltavaa käyttää ainoastaan 64-bittisiä prosessoreita Windows Home Serverin kanssa, jotta tulevaisuudessa uusiin versioihin päivittäminen onnistuisi. (Edney 2007, 7).

3.2 Amahi Home Server

Amahi Home Serverin idea on sama kuin Windows Home Serverin. Ne eroavat toisistaan vain lähinnä arkkitehtuuriltaan ja ominaisuuksiltaan. Amahi Home Server pohjautuu ainakin toistaiseksi Fedora Linux -käyttöjärjestelmään. Tuki Ubuntulle on tulevaisuudessa mahdollinen.

Kehittäjät kutsuvat järjestelmäänsä nimellä HDA eli Home Digital Assistant. Amahi Home Serverissä ei ole WHS:n tapaista hallintakonsolia, vaan hallinta tapahtuu web-selaimen kautta Amahi Dashboardissa. Amahi Home Server on ilmainen, koska se perustuu avoimeen lähdekoodiin. (Features Of The Amahi Home Server, hakupäivä 8.2.2010).

3.2.1 Ominaisuudet

AHS:ssä on myös paljon hyödyllisiä ominaisuuksia. Se sisältää digitaalisen musiikin tai muun audion streamauksen kaikkiin verkkoon kytkettyihin laitteisiin AmahiTunes – ohjelmalla, joka sisältää Firefly mediapalvelimen. (Feature Gallery for the Amahi Home Server, hakupäivä 14.2.2010).

Omat palvelut, kuten DHCP-integroitu (Dynamic Host Configuration Protocol) dynaaminen DNS (Domain Name System), web-palvelin sekä NAS-palvelimet (Network Access Storage) ovat helposti hallinnoitavissa. Mukana tulee esiasennettu OpenVPN pelkkä asiakasohjelma riittää VPN:n (Virtual Private Network) käyttämistä varten. (Feature Gallery for the Amahi Home Server, hakupäivä 14.2.2010).

Tiedostonjako on tehty helpoksi kotiverkon tietokoneita varten ja kovalevyjä varten on omat monitorointityökalut. Varmuuskopiointi on helppoa ja mahdollistaa päivittäisten varmuuskopiointien tekemisen ja myös kovalevykloonauksen on mahdollista tehdä. (Feature Gallery for the Amahi Home Server, hakupäivä 14.2.2010).

Amahi Home Serveriin on mahdollista rakentaa oma Private Wiki – sivusto joko henkilökohtaiseen tai pienen työryhmän käyttöön. Siinä on myös selkeät kalenterit, joita voi käyttää web-käyttöliittymän kautta sekä tuki Windowsin Vistan kalenterin synkronointiin. (Feature Gallery for the Amahi Home Server, hakupäivä 14.2.2010).

Sisäänrakennettu hakutoiminto mahdollistaa tuen selaimille, kuten Firefoxille ja Internet Explorer 7:lle. Modulaarinen ohjelmistoarkkitehtuuri tukee AJAX-ohjelmien (Asynchronous JavaScript and XML) helppoa asentamista. Dynaamisella DNS-palvelulla voidaan pitää esimerkiksi omaa web-palvelinta tai sallia yhteyksiä etäkäyttöä varten. (Feature Gallery for the Amahi Home Server, hakupäivä 14.2.2010).

3.2.2 Lisäominaisuudet (Apps)

Myös Amahi Home Serverin toiminallisuutta voidaan laajentaa Amahi Dashboardista löytyvästä Apps-osiosta. Amahissakaan ei ole oletuksena muuta kuin lähinnä perusominaisuuksia, joilla palvelimen toimintaa hallitaan.

Apps-osio tarjoaa monipuolisen listan ladattavista ohjelmista, joilla voidaan lisätä käteviä lisäominaisuuksia. Sieltä löytyy esimerkiksi oman domainin lisäys, etähallintatyökaluja ja streamaus-palveluita.

3.2.3 Järjestelmävaatimukset

Amahi Home Serverin järjestelmävaatimukset eivät ole myöskään nykymittapuun mukaan kovin vaativia (Kuvio 3). Suositeltuja vaatimuksia ei ole, mutta todellisuudessa kotipalvelimeksi tarkoitettu järjestelmä tarvitsee kuitenkin kovalevytilaa paljon enemmän kuin minimivaatimus kertoo. Lisäksi on huomioitava muutkin minimitehot, jotka eivät välttämättä riitä pyörittämään palvelinta mahdollisimman jouhevasti.

KUVIO 3. Amahin Home Serverin järjestelmävaatimukset

Vaatimukset	Minimi	Suositus
Proessori	800 MHz Pentium 3 (tai vastaava)	-
Muisti	512 MB	-
Kovalevytila	4 GB	-
Verkko	-	-

4 TESTAUSSUUNNITELMA

Testauksen kohteena ovat Windows Home Server sekä Amahi Home Server – kotipalvelinkäyttöjärjestelmät. Testauksen tavoitteena on tutkia ja selvittää, kumpi näistä vaihtoehdoista on parempi kotikäyttöön tutkien ominaisuuksia, käytettävyyttä sekä toiminnallisuutta. Työssä on otettu myös huomioon se, että Windows Home Server on maksullinen, kun taas Amahi Home Server on ilmainen.

Testausympäristö koostuu laitteistosta, johon kuuluu palvelinkone, yksi pöytäkone, yksi kannettava tietokone sekä langaton reititin. Palvelinkoneessa on asennettuna Windows Home Server sekä Amahi Home Server. Asiakaskoneissa on asennettuna Windows 7 –käyttöjärjestelmä.

Verkkoyhteydet hoitaa langaton reititin, joka on yhteydessä ulkoverkkoon VDSL-modeemin kautta. Kannettava tietokone on yhteydessä verkkoon langattomalla (WLAN) ja muut langallisella (RJ45) yhteydellä. Reititin jakaa lähiverkon tietokoneille DHCP:llä omat sisäverkon IP-osoitteet ja yhdistää ne ulkoverkkoon yhden ulkoisen IP-osoitteen kautta.

Ohjelmistoihin kuuluvat Windows Home Server, Amahi Home Server, Fedora 12, Windows 7, Nessus–testaustyökalu sekä lukuisia muita järjestelmiin liittyviä apuohjelmia. Nessus–testaustyökalua esitellään tarkemmin tässä kappaleessa.

Järjestelmien asennusten jälkeen konfiguroimme molemmat järjestelmät toimintakuntoon, jonka jälkeen pääsemme testaamaan ominaisuuksia, käytettävyyttä sekä toiminnallisuutta. Näiden toimintojen jälkeen suoritamme lisäksi tietoturvatestejä, jotka tehdään Nessus–testaustyökalulla. Lopuksi pohdimme molempia järjestelmiä näiden tekijöiden pohjalta.

Tärkeimpiä kriteereitä ovat ominaisuudet, käytettävyys ja toiminnallisuus yleisellä tasolla sekä asennuksen helppous. Lisäksi tutkimme järjestelmien lisäominaisuuksia (Add-ins), etähallintaa ja tietoturvaa. Lisäkritereinä mainittakoon, että toinen järjestelmä on maksullinen ja toinen ilmainen.

Tietoturvallisuutta testaamme Nessus-testaustyökalulla, joka on Teneble-yhtiön tekemä tehokas ja ajan tasalla pysyvä tietoturvaskanneri, joka pyrkii selvittämään, onko annetun verkko-osoitteen tai verkko-osoiteavaruuden kohteeseen mahdollista tehdä tietomurto. Sillä voidaan testata turvallisuutta eri tavoin pluginien (erilaisia sisäisiä testiohjelmia) avulla eli voidaanko murto tehdä ihmisen tai esimerkiksi jonkin haittaohjelman, kuten madon tai viruksen toimesta. (Nessus Tietoturvan tarkastamisohjelma, Hartikainen, hakupäivä 24.3.2010.).

Nessus perustuu palvelin-asiakas –teknoologiaan. Palvelimet voivat sijaita periaatteessa missä tahansa, joten testejä voidaan ajaa verkkoa ajatellen monista eri paikoista. Esimerkiksi keskitetty asiakas tai hajautetut asiakkaat voivat hallita kaikkia palvelimia. Nessus-palvelin suorittaa varsinaisen testin, kun taas asiakas hoitaa asetukset ja raportoinnin. (Introduction to Nessus, Anderson, hakupäivä 2.4.2010).

5 KOTIPALVELINKÄYTTÖJÄRJESTELMIEN ASENNUS

Ennen kuin asentaminen aloitetaan, on hyvä tarkastaa, että palvelin on valmis siihen. Asentamiseen tarvitaan tietysti näppäimistö, hiiri sekä näyttö. Lisäksi BIOS-asetuksissa olevan käynnistysjärjestyksen on oltava oikein, jotta palvelin osaa käynnistää asennuksen DVD-levyltä. Monessa koneessa nämä asetukset ovat kuitenkin oletuksena niin, että DVD-levy käynnistyy automaattisesti.

Jos näin ei ole ja DVD-levy ei käynnisty, BIOS-asetuksiin pääsee koneesta riippuen yleensä joko näppäimillä F2, Del tai Insert heti sen käynnistyessä. Etsimällä kohdan Boot Order tai Boot Priority löytää käynnistysjärjestyksen, joka tulee olla niin, että CD-ROM tai DVD-ROM on listan järjestyksessä ennen kiintolevyä (Hard Drive). Lopuksi asetukset tulee tallentaa valitsemalla Save and Exit, Exit Saving Changes tai muu samankaltainen kohta. Kun kone on käynnistynyt uudelleen, DVD-levyn pitäisi käynnistyä normaalisti.

5.1 Windows Home Server

Windows Home Serverin asennus ei käynnisty automaattisesti, vaan käyttäjää pyydetään painamaan mitä tahansa nappia, jotta asennusohjelma käynnistyy. Ohjelma lataa asennustiedostoja, jonka jälkeen päästään varsinaiseen asennusohjelmaan.

1. Kun asennusohjelma on käynnistynyt, ruutuun tulee Welcome to Windows Home Server Setup -ikkuna. Tässä vaiheessa ei voi tehdä vielä mitään määrittäksiä, joten jatketaan asennusta normaalisti eteenpäin painamalla Next.
2. Seuraavaksi käyttäjää pyydetään valitsemaan kiintolevy, mihin Windows Home Server asennetaan. Listassa pitäisi näkyä kaikki kiintolevyt mitä palvelimeen on asennettu. Kun kiintolevy on valittu, painetaan Next.

3. Asennus kysyy minkä tyyppisen asennuksen käyttäjä haluaa tehdä. Tyypiksi valitaan New Installation eli uusi asennus, koska järjestelmä halutaan asentaa puhtaasti alusta alkaen. Vaihtoehtoisesti käyttäjä voi valita järjestelmän palautuksen, mikäli esimerkiksi toisella kiintolevyllä olisi Windows Home Serverin tiedostoja. Painetaan Next.
4. Tämän jälkeen pyydetään myös kieli- ja näppäimistöasetuksia, jotka valitaan pudotusvalikoista. Tässä tapauksessa asetuksiin laitetaan kumpaankin kohtaan Suomi. Jatketaan Next-painikkeella.
5. Seuraavaksi asennus näyttää EULA-tiedot (End-User License Agreement), jotka kertovat mihin sopimusehtoihin käyttäjän on suostuttava. Mikäli sopimusehtoja ei hyväksytä, asennus peruuntuu. Valitaan "I accept the agreement" ja painetaan Next.
6. Seuraavassa ikkunassa syötetään 25-merkkinen lisenssiavain. Kun lisenssiavain on syötetty, jatketaan painamalla Next-painiketta.
7. Käyttäjällä on mahdollisuus nimetä palvelin haluamansa mukaisesti. Oletuksena nimi on Server, joka käy tietysti hyvin palvelimen nimeksi, mikäli käyttäjä aikoo pitää vain yhtä palvelinta kotiverkossaan. Painetaan Next-painiketta asennuksen jatkamiseksi.
8. Palvelimen nimeämisen jälkeen tulee eteen ikkuna, jossa on vielä mahdollisuus muuttaa kiintolevyä, johon Windows Home Serverin asennetaan. Jatkaaksesi asennusta on valittava "I acknowledge that all data on these drives will be lost", joka tarkoittaa, että valittu kiintolevy alustetaan. Jatketaan Next-painikkeella.
9. Tässä vaiheessa kaikki tarpeelliset määrytykset asennuksen suorittamiseksi on tehty. Lopuksi tulee ikkuna, jossa ilmoitetaan, että asennus on valmis aloitettavaksi. Aloitetaan asennus painamalla Start-painiketta.

10. Kun asennusprosessi on suoritettu, ruutuun tulee Welcome-ruutu, josta päästään eteenpäin painamalla Welcome-painiketta. Tämän jälkeen käyttäjää pyydetään syöttämään salasana sekä salasanavihje (Kuvio 4). On suositeltavaa käyttää salasanaa, joka on vahva mutta kuitenkin helposti muistettava. Hyvä salasana sisältää pieniä ja isoja kirjaimia sekä numeroita ja on pituudeltaan vähintäänkin 8-merkkiä. Turvallinen salasana sisältää ainakin 14-merkkiä. Painetaan Next-nuolipainiketta.

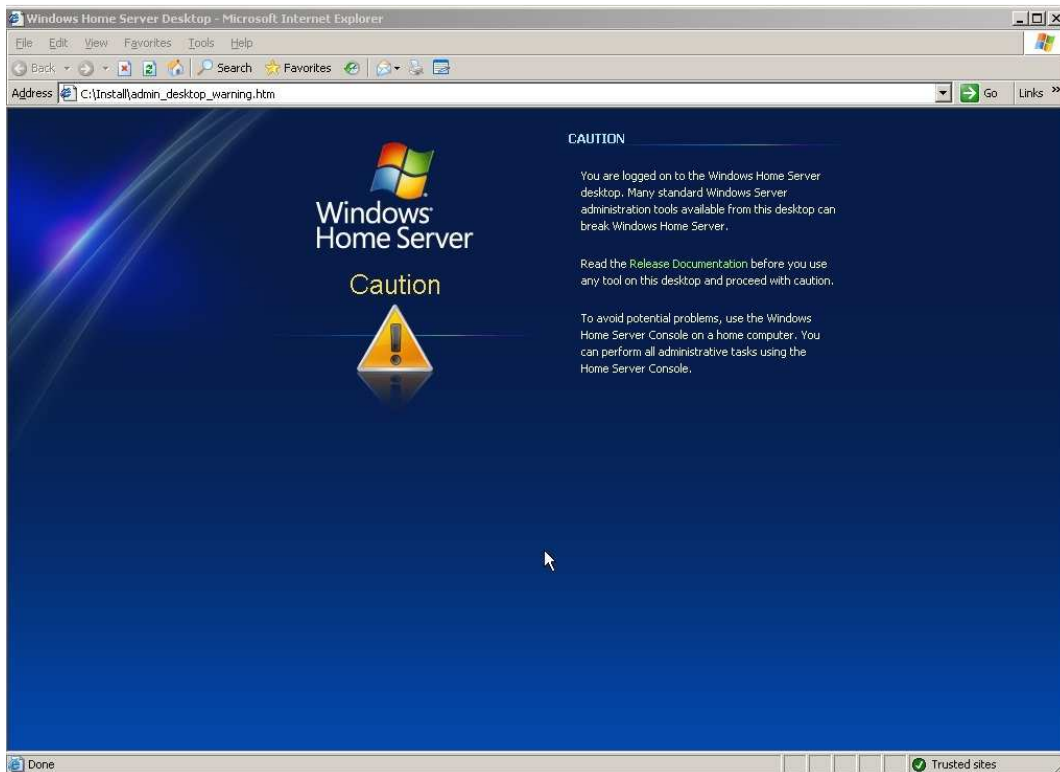


KUVIO 4. Salasanan määrittäminen

11. Salasanan kyselykohdan jälkeen käyttäjää pyydetään valitsemaan automaattiset päivitykset palvelimelle. On suositeltavaa jättää oletusvalinta, jotta päivitykset ajetaan automaattisesti palvelimeen. Jatketaan Next-nuolipainikkeella.

12. Tämän jälkeen kysytään vielä haluaako käyttäjä osallistua asiakaskyselyihin sekä virheraportointiin. Valitaan joko Yes tai No ja painetaan Next-nuolipainiketta.

13. Viimeistellään asennus Continue-painikkeella. Ruutuun ilmestyy aivan normaalin näköinen Windows-työpöytä ja selaimen varoitusikkuna (Kuvio 5), jolloin käyttöjärjestelmä on asennettu onnistuneesti.



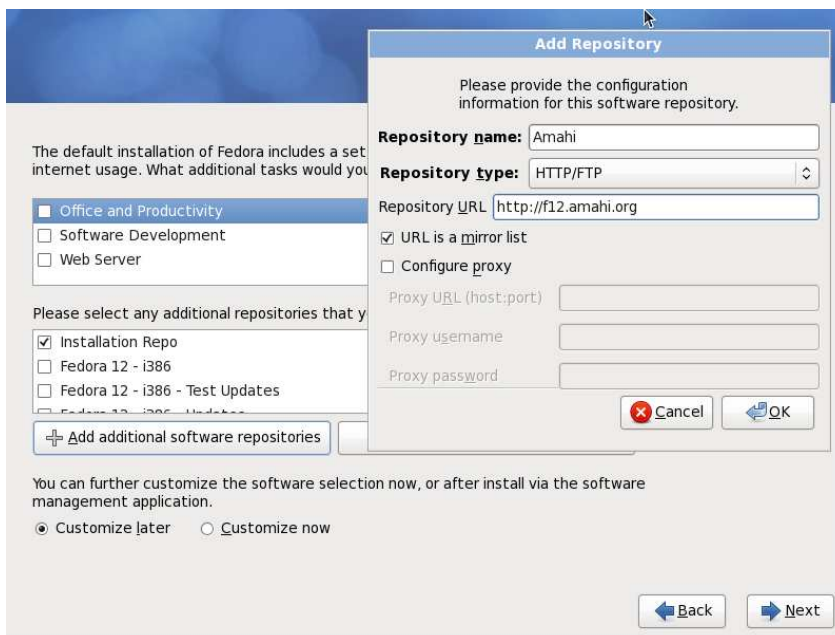
KUVIO 5. Varoitusikkuna

5.2 Amahi Home Server

Ennen aloittamista on huomioitava, että asennusta varten tarvitaan Fedora 12 Install DVD -asennuslevy, jonka voi ladata osoitteesta <http://mirrors.fedoraproject.org/publiclist/Fedora/12/>. Asennuslevy täytyy polttaa DVD-levylle image-tiedostosta. Internet-yhteys tulee olla palvelinkoneeseen koko asennuksen ajan. Jos palvelinkoneessa on useampi NIC (Network

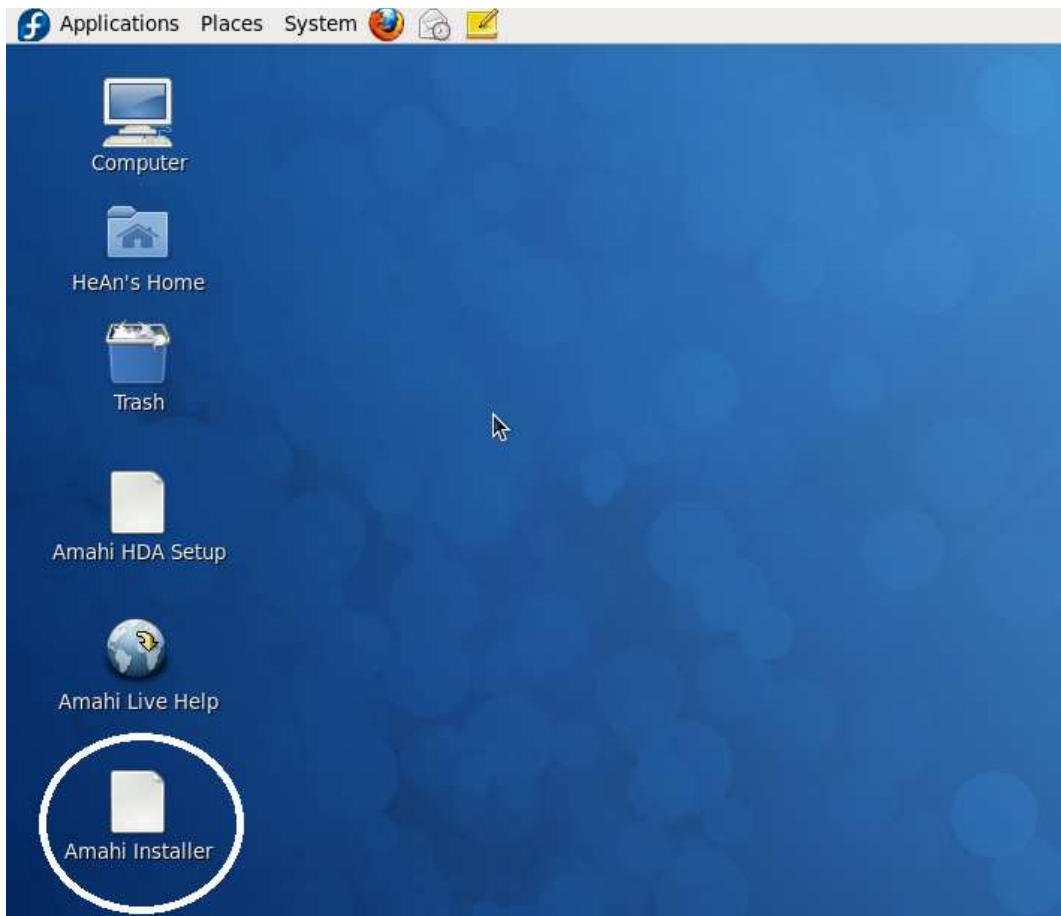
Interface Card) eli verkkokortti, on huomioitava, että asennus tukee vain ensimmäistä verkkokorttia (eth0), joten verkkokaapeli tulee olla kytkettynä siihen. DVD-levy käynnistyy automaattisesti koneen käynnistyessä.

1. Kun DVD-levy on käynnistynyt, tulee hetken kuluttua ruutu, josta valitaan ensimmäinen vaihtoehto eli Install or Upgrade existing system.
2. Seuraavaksi eteen tulee asennusohjelma, jossa edetään painamalla Next.
3. Syötetään isäntänimi lähiverkkoa varten ja painetaan Next.
4. Asetetaan salasana root-tiliä varten ja jatketaan painamalla Next.
5. On suositeltavaa ruksata valinta Office and Productivity pois, mikäli palvelinta ei halua käyttää samanaikaisesti työasemana. Painetaan Add additional software repositories, jolloin aukeaa uusi ikkuna (Kuvio 6), johon syötetään Repository nameksi Amahi, valitaan tyyppiä HTTP/FTP ja osoitteeksi http://f12.amahi.org. Painetaan OK.



KUVIO 6. Amahin asennuspakettien määrittäminen

6. Tämän jälkeen asennusohjelmaa kysyy verkkosovitinta (eth0), jossa annetaan olla oletusasetuksina DHCP ja IPv4 päällä. Hyväksytään painamalla OK ja painetaan Next.
7. Kun asennus on suoritettu loppuun, käynnistetään kone uudelleen painamalla Reboot. DVD-levy tulee poistaa asemasta ennen uudelleen käynnistystä.
8. Eteen tulee Welcome-ruutu, josta jatketaan painamalla Forward.
9. Käyttäjälle esitetään lisenssitiedot, josta edetään painamalla Forward.
10. Seuraavaksi luodaan tavallinen käyttäjä syöttämällä nimi, käyttäjänimi ja salasana. Painetaan Forward.
11. Määritellään päivämäärä- ja aika-asetukset ja painetaan Forward.
12. Lopuksi asennus kysyy käyttäjältä halutaanko lähettää Fedora Projektia varten laitteistotiedot. Viimeistellään painamalla Finish.
13. Kirjaututaan sisään, jolloin eteen ilmestyy Fedoran työpöytä.
14. Tupla-klikataan työpöydältä löytyvää Amahi Installer –kuvaketta (Kuvio 7), jolloin eteen aukeaa selainikkunaan Amahi Installer –sivusto.



KUVIO 7. Amahin asennuskuvake

15. Syötetään Install Code ja painetaan Submit. Koodin saa rekisteröidyttyään Amahin sivuilla osoitteessa <https://www.amahi.org/signup/>.

16. Lopuksi on suositeltavaa käynnistää järjestelmä uudestaan, jotta kaikki toimii oikein.

17. Uudelleenkäynnistyksen jälkeen Amahi on käyttövalmis. Kirjaudutaan Amahi Dashboardiin Fedoran käyttäjätunnuksilla.

6 KÄYTTÖÖNOTTO JA KONFIGUROINTI

Otamme käyttöön kotipalvelinkäyttäjärjestelmät ja esittelemme niiden käytettävyyttä ja hallittavuutta konfiguroimalla ne varsinaiseen toimintakuntoon. Työssä ei esitellä varsinaisesti mitään erikoisempia säätöjä, vaan lähinnä konfiguroinnit, joilla saadaan palvelinten perustoiminnot kuntoon.

On tietenkin käyttäjästä itsestään kiinni, minkälaisia toimintoja palvelimeen halutaan räätälöidä. Molempiin palvelinkäyttäjärjestelmiin on mahdollista lisätä toiminnallisuuksia melko laajasti. Tekemillämme peruskonfiguroinneilla saadaan kuitenkin palvelinten perusidea ja käyttökohteet selville.

6.1 Windows Home Server

Käyttäjärjestelmän asennuksen jälkeen palvelin otetaan varsinaisesti käyttöön ja siihen tehdään tarvittavat konfiguroinnit, jotta se saadaan kunnan toimintakuntoon. Ensiksi kannattaa kuitenkin tarkistaa toimiiko Ethernet-yhteys oikein. Mikäli verkkolaitteet ja kaapelointi ovat kunnossa, pitäisi porttivalon palaa kiinteästi joko kytkimessä, reitittimessä tai modeemissa, riippuen mihin näistä palvelin on kytketty. Windows Home Server hakee asennuksen jälkeen uusimmat päivitykset järjestelmään automaattisesti.

WHS:ää hallitaan Windows Home Server Consolen kautta, jonne päästään asiakaskoneiden työpöydiltä sijaitsevilta pikakuvakkeilta. Consoleen päästää lisäksi myös etäyhteydellä selaimen kautta ja tietysti myös palvelimen päästä.

6.1.1 Kotitietokoneen liittäminen palvelimeen (Windows Home Server Connector)

Mikäli kaikki perusasiat ovat kunnossa palvelimen suhteen, on aika yhdistää kotitietokoneet palvelimeen. Tämä onnistuu suoraan CD-levyllä olevan Connector –ohjelman avulla, joka tulee Windows Home Serverin mukana.

On myös mahdollista ladata ohjelmisto palvelimen jaetuista kansioista, jonka polku on \\Server\Software\Home Server Connector Software\, jonne pääsee esimerkiksi Windows Home Serverin Resurssienhallinnalla. On huomioitava, että asennus täytyy ajaa asiakaskoneessa, ei palvelimessa. Tällöin palvelimelta haettu ohjelmisto on syytä siirtää esimerkiksi USB-muistitikulle. Jos käyttäjänimeä ja salasanaa pyydetään, on käyttäjänimi Administrator ja salasana palvelimen oma salasana. Asennus etenee seuraavanlaisesti:

1. Aloitusikkunan avauduttua painetaan Next.
2. Sopimusehdot hyväksytään ja painetaan Next, jolloin asennus alkaa.
3. Asennuksen jälkeen syötetään Windows Home Serverin salasana, joka annettiin asennusvaiheessa (Kuvio 8). Jatketaan Next-painikkeella.



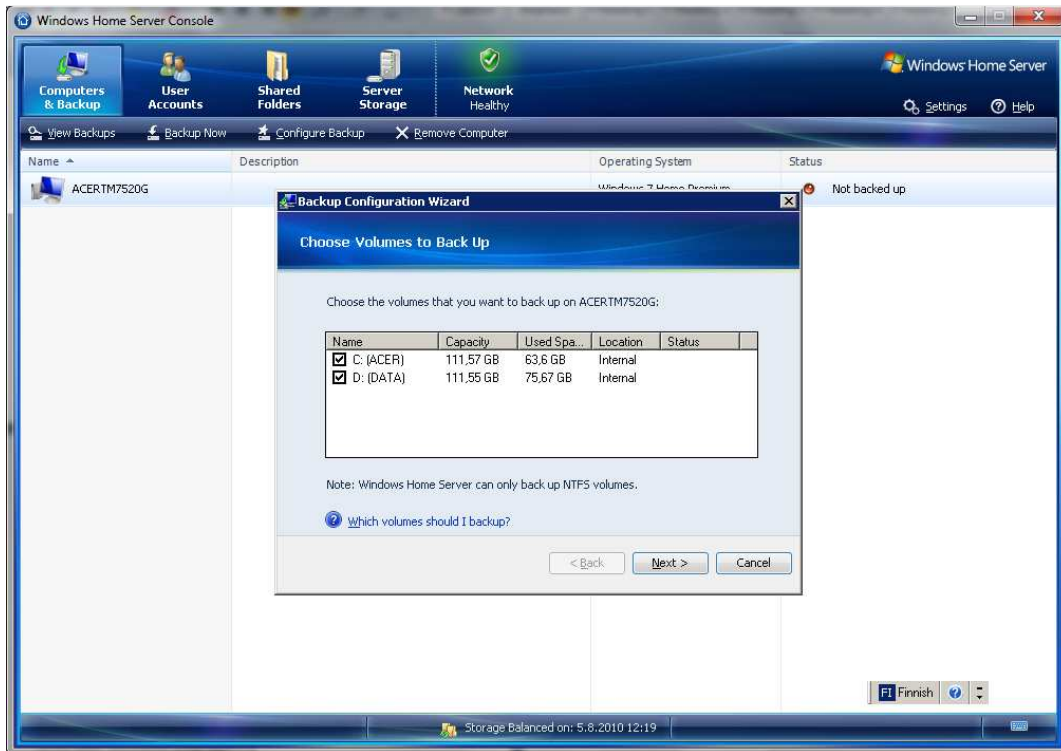
KUVIO 8. Windows Home Serverin salasana kirjautumista varten

4. Seuraavaksi voidaan valita herätetäänkö tietokone varmuuskopiointiin ajaksi. Valinnan jälkeen painetaan Next, jolloin Windows Home Server Connector yhdistää tietokoneen palvelimeen.
5. Painetaan Next asennuksen viimeistelemiseksi.
6. Lopuksi painetaan vielä Finish, jonka jälkeen työpöydälle ilmestyy pikakuvake, josta pääsee palvelimella sijaitseviin jakokansioihin ja toinen pikakuva, josta päästään Windows Home Server Consoleen.

6.1.2 Varmuuskopioiden hallinta (Computers & Backup)

Windows Home Server Consolessa sijaitsevalla Computers & Backup – välilehdellä voi asettaa ja määrittellä varmuuskopiointeja kotiverkon tietokoneille ja nähdä myös listan palvelimeen kytketyistä tietokoneista.

1. Valitaan haluttu tietokone listasta, jolle halutaan määrittää varmuuskopioinnit.
2. Painetaan Configure Backup, jolloin Backup Configuration Wizard – ikkuna aukeaa. Painetaan Next.
3. Seuraavaksi täytyy valita haluttu levyosio, jolle varmuuskopiointi tehdään. (Kuvio 9). Edetään painamalla Next-painiketta.



KUVIO 9. Varmuskopioitavan osion valinta

4. Määritellään kansiot, mitkä halutaan jättää varmuuskopioinnista pois. Mikäli mitään kansioita ei oteta pois, palvelin varmuuskopioi tietokoneen levyosion kokonaan. Painetaan Next.
5. Viimeistellään ohjattu toiminto painamalla Done-painiketta.

6.1.3 Käyttäjän lisääminen (User Accounts)

Käyttäjien lisääminen tapahtuu Home Server Consolessa, jonka voi käynnistää Start-valikon All Programs –kohdasta. Mikäli käyttäjän lisääminen tehdään asiakaskoneesta, täytyy Windows Home Server Consoleen syöttää salasana ja painaa Connect-painiketta, jolloin konsoli-ikkuna avautuu. Käyttäjä lisätään seuraavanlaisesti:

1. Painetaan User Accounts -välilehteä.

2. Painetaan Add, jolloin Add User Account –ikkuna avautuu (Kuvio 10).



KUVIO 10. Käyttäjän lisääminen

3. Syötetään käyttäjän etu- ja sukunimi sekä käyttäjätunnus (Logon name).
4. Mikäli käyttäjälle halutaan antaa oikeudet etäyhteyttä varten, ruksataan valinta Enable Remote Access for this user.
5. Edetään painamalla Next, jonka jälkeen pyydetään syöttämään salasana käyttäjätiliä varten (Kuvio 11).

On huomioitava, että käyttäjätilien tunnukset kannattaa olla samat kuin asiakaskoneiden käyttäjätunnukset. Tämä edesauttaa jakokansioiden oikeuksien toimivuuden varmemmin ja lisää käytettävyyttä, koska jakokansioihin pääsee lähiverkon kautta suoraan syöttämättä erikseen käyttäjätunnuksia.



KUVIO 11. Käyttäjätilin salasana

6. Painetaan Next, jonka jälkeen voidaan määrittellä käyttäjän oikeudet jakokansioihin (Kuvio 12).



KUVIO 12. Oikeudet jakokansioihin

7. Jokaiselle kansiolle voidaan määrittää halutut oikeudet: Full, Read tai None.
8. Viimeistellään käyttäjän lisääminen painamalla Finish, jonka jälkeen käyttäjä on lisätty palvelimelle. Käyttäjälle on nyt annettu myös oikeudet määriteltäviin kansioihin sekä lisätty oma käyttäjäkohtainen kansio.
9. Painetaan lopuksi vielä Done.

6.1.4 Jakokansiot (Shared Folders)

Shared Folders –välilehdellä näkyvät jaettavat ja käyttäjien omat kansiot. Jakokansioita on mahdollista lisätä, muokata, poistaa ja katsella. Jakokansioita lisätään seuraavanlaisesti:

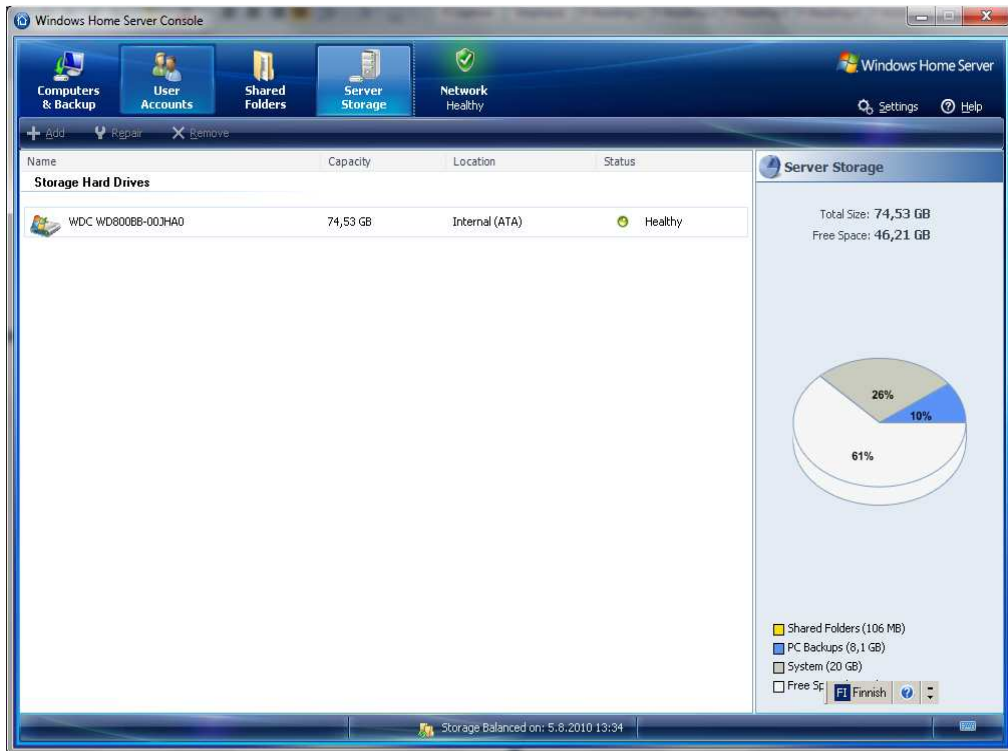
1. Painetaan Add-painiketta, jolloin eteen aukeaa Shared Folder –ikkuna (Kuvio 13).



KUVIO 13. Jakokansion lisääminen

2. Syötetään jakokansion nimi.
3. Halutessaan voidaan syöttää kuvaus kansiota varten.
4. Enable Folder Duplication kannattaa valita, mikäli halutaan, että Windows Home Server tekee kyseisen kansion tiedostoista kopiot. Tällöin palvelimessa täytyy olla vähintään kaksi kiintolevyä. Jatketaan painamalla Next.
5. Käyttäjää pyydetään asettamaan käyttöoikeudet kyseiseen kansioon.
6. Painetaan Finish, jonka jälkeen Windows Home Server luo kansion, asettaa käyttöoikeudet ja ottaa käyttöön duplikoinnin, mikäli mahdollista. Uuden jakokansion pitäisi näkyä Shared Folders –välilehdellä.
7. Viimeistellään painamalla Done.

Server Storage –välilehdellä näkyy palvelimen kiintolevyt, joita voidaan lisätä, poistaa ja korjata. Lisäksi ikkunan oikeassa reunassa näkyy kiintolevyjen käyttökapasiteetti sekä mitkä resurssit syövät eniten tilaa (Kuvio 14). Mikäli käytössä on vain yksi kiintolevy, WHS pystyy tallentamaan kaikki tiedostot pelkästään siihen. Tällöin duplikaattien tekeminen tiedostoista ei ole mahdollista, koska se vaatii käyttöönsä vähintään kaksi kiintolevyä. Tilanhallinnassa ei myöskään pysty tekemään mitään lisäyksiä, poistoja tai korjauksia.



KUVIO 14. Palvelimen tilanhallinta

6.1.5 Verkon monitorointi (Network Healthy)

Windows Home Serverissä verkon monitorointi on tehty yksinkertaiseksi. Konsolissa näkyvä Network Healthy –kuvake (Kuvio 15) ilmoittaa kotiverkon tilan erilaisilla väreillä. Vihreä tarkoittaa, että verkko on suojattu ja kunnossa eli kaikki asiakaskoneet ovat varmuuskopioitu, niiden turva-asetukset ovat oikein ja Windows Home Serveriin on asennettu kaikki päivitykset. Sininen kertoo, että palvelin tekee varmuuskopiota asiakastietokoneesta. Oranssi tarkoittaa, että kotiverkossa voi olla jokin ongelma, kuten esimerkiksi epäonnistunut varmuuskopiointi. Punainen kuvastaa, että kotiverkossa on vakava ongelma, joka voi johtua esimerkiksi siitä, että Windows Home Serverin päivitykset eivät ole ajan tasalla tai jossakin asiakastietokoneessa ei ole palomuuuri päällä. Harmaa tarkoittaa, että asiakaskone ei löydä Windows Home Serveriä, joka voi johtua esimerkiksi siitä, että verkkokaapeli voi olla irti.



KUVIO 15. Verkon tilasta kertova kuvake

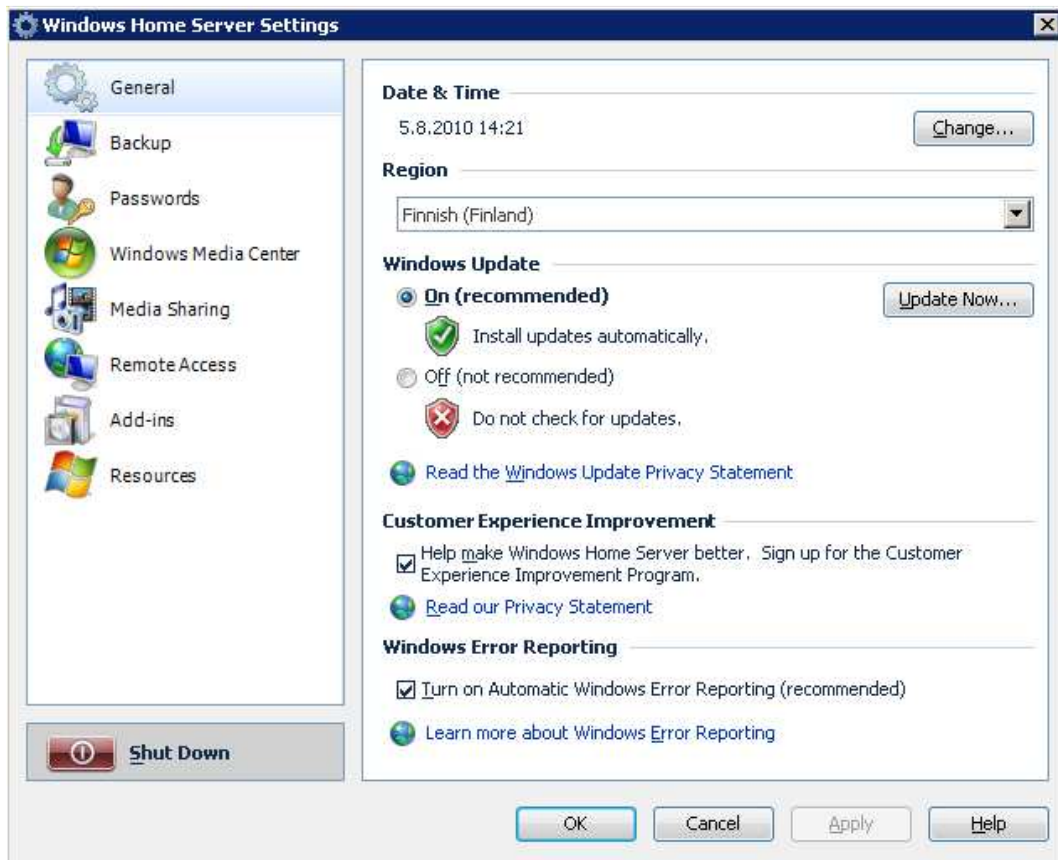
Asiakastietokoneissa näkyvät myös nämä samat ilmoitukset, jotka löytyvät tehtäväpalkin oikeassa reunassa olevasti Windows Home Server –kuvakkeesta. Kuvakkeeseen tulee teksti, joka ilmoittaa kotiverkon tilan jos jotain muutoksia tapahtuu (Kuvio 16).



KUVIO 16. Kuvakkeen kertoma tila

6.1.6 Palvelimen järjestelmäasetukset (Settings)

Palvelimen järjestelmäasetuksiin (Kuvio 17) päästään Windows Home Server Consolesta löytyvästä Settings-painikkeesta. General-välilehdellä voidaan määrittellä aika- ja päivämääräasetukset, millä alueella palvelin sijaitsee, automaattiset päivitykset, asiakaskokemuspalautteen sekä Windowsin virheraportoinnin.



KUVIO 17. Järjestelmäasetukset

Backup-välilehdellä voidaan määrittellä varmuuskopiointin aloitus- ja loppu ajankohdat sekä kuinka monta kuukautta, viikkoa ja päivää säilytetään varmuuskopiointit. Vanha varmuuskopio poistetaan aina uuden varmuuskopiointin aikana.

Passwords-välilehdeltä voidaan vaihtaa Windows Home Serverin salasana sekä määrittää käyttäjien salasana vahvuuden.

Windows Media Center –kohdasta määritellään jaettavien kansioden oikeudet Windows Media Center –ohjelmaa varten.

Media Sharing –välilehdellä voi määrittellä, jaetaanko palvelimella olevat musiikki-, kuva-, ja videokansiot kotiverkon laitteille streamausta varten.

Remote Access –välilehdeltä voidaan asettaa Windows Home Serverin etäyhteystoiminto päälle. Tällöin Windows Home Serveriä varten luodaan

automaattisesti oma Internet-sivusto. Remote Access -toiminnosta kerrotaan tarkemmin seuraavassa kappaleessa.

Add-ins -välilehdellä palvelimeen voidaan asentaa lisäominaisuuksia, jotka laajentavat Windows Home Serverin toiminnallisuutta. Asennettu lisäominaisuus näkyy uutena välilehtenä konsoli-ikkunassa.

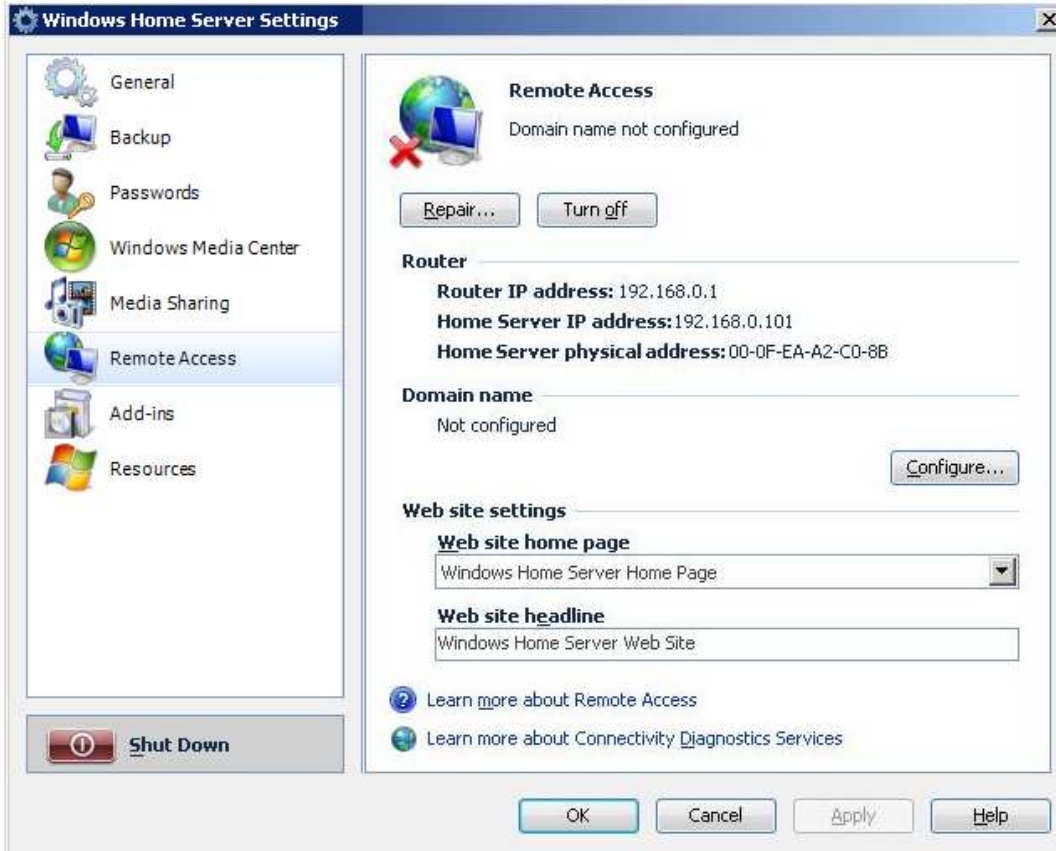
Viimeisenä oleva Resources kertoo erilaisia tietoja palvelimesta, kuten käyttöjärjestelmän version, palvelinkoneen tiedot sekä eri ohjelmistojen versiotiedot. Lisäksi sieltä päästään Windows Home Serverin tukipalveluihin.

6.1.7 Etäyhteyden määrittely (Remote Access)

Etäyhteyttä varten täytyy Windows Home Serveriin määrittellä Remote Access -palvelu, joka tarkoittaa käytännössä sitä, että palvelimelle täytyy määrittää oma domain eli verkko-osoite ja tehdä reitittimeen manuaalisesti tarvittavat porttiasetukset yhteyksiä varten.

UPnP-protokollan (Universal Plug and Play) käyttäminen mahdollistaa automaattisen konfiguroinnin tekemisen reitittimeen (mikäli se tukee kyseistä protokollaa), jolloin porttiasetuksia ei tarvitse tehdä manuaalisesti. UPnP:n käyttö ei ole tietoturvalisistä syistä kuitenkaan niin suositeltavaa. Porttiasetuksien laittamisesta kerrotaan omassa kappaleessaan. Etäyhteys kytketään päälle seuraavanlaisesti:

1. Painetaan konsolista löytyvää Settings-painiketta. Valitaan Remote Access -välilehti (Kuvio 18).



KUVIO 18. Remote Access -välilehti

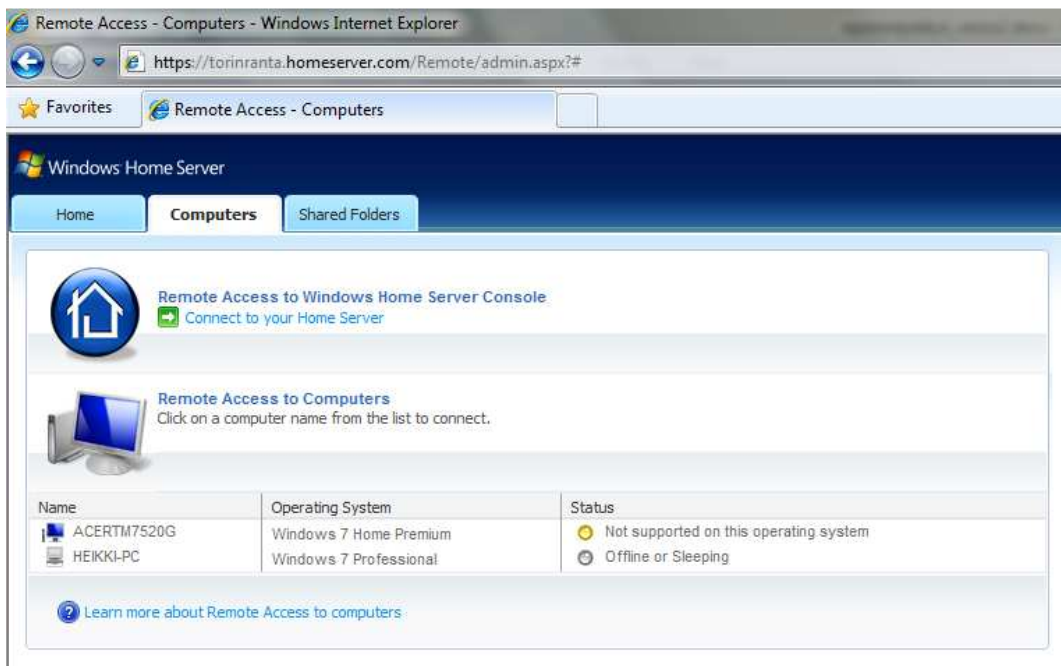
2. Domain name –kohdasta Configure-painiketta painamalla saadaan päälle Domain Name Setup –ikkuna.
3. Painetaan Next, jolloin käyttäjää pyydetään syöttämään Windows Live ID –tunnukset.
4. Syötetään haluttu alidomainin nimi ja painetaan Confirm-painiketta, jolloin tehdään tarkistus onko osoite vapaana. Mikäli osoite on vapaana, näkyviin tulee vihreä pukki ja näyttää täydellisen verkko-osoitteen. Painetaan Finish.
5. Viimeistellään domainin tekeminen Done-painikkeella, jonka jälkeen ikkuna sammuu automaattisesti ja uutta verkko-osoitetta testataan. Painetaan OK.

6.1.8 Etäyhteyden käyttäminen (HTTP Remote Access)

Palvelimeen pääsee käsiksi myös etäyhteyden kautta millä tahansa tietokoneella mistä päin maailmaa tahansa. Tämä onnistuu kirjautumalla palvelimen sivuille omilla käyttäjätunnuksilla. Käyttäjälle täytyy olla määritettyä etäyhteysoikeudet.

Home-välilehti kertoo Remote Accessin toiminnoista, Computer-välilehdeltä pääsee konsoliin ja muihin kotiverkon tietokoneisiin ja Shared Folders –kohdasta löytyy palvelimella sijaitsevat jakokansiot, joihin voidaan lisätä ja ladata tiedostoja sekä poistaa niitä. Konsoliin pääsee seuraavanlaisesti:

1. Kun palvelimen sivuille on kirjaututtu, painetaan Computers-välilehteä (Kuvio 19).



KUVIO 19. Etähallinnan Computers –välilehti

2. Painetaan Connect to your Home Server –linkkiä, jonka jälkeen käyttäjää pyydetään syöttämään palvelimen salasana.
3. Eteen tulee ikkuna, joka kysyy luotetaanko palveluun. Painetaan Connect, jolloin selainikkunaan ilmestyy Windows Home Server Console.
4. Kun etäyhteys-istunto halutaan lopettaa, painetaan vasemmasta yläreunasta löytyvää Disconnect-painiketta.

6.1.9 Palvelimen turvallisuus

Windows Home Serverin mukana tulee oma sisäinen palomuuuri, joka on riittävän turvallinen useimmille käyttäjille. Lisäksi reititin suojaa omalta osaltaan palvelinta ja kotiverkkoa. Turvallisuutta voidaan kuitenkin aina parantaa.

Windows Home Serverin, kuten ei muidenkaan käyttöjärjestelmien mukana tule lainkaan virustorjuntaohjelmistoa. Tähän ongelmaan on olemassa muutamia kaupallisia ratkaisuja, kuten avast! Windows Home Server Edition ja F-Secure Home Server Security 2009. Myös pari ilmaista sovellusta on tarjolla tällä hetkellä, joista käyttöönottoon suositeltava on ClamWin.

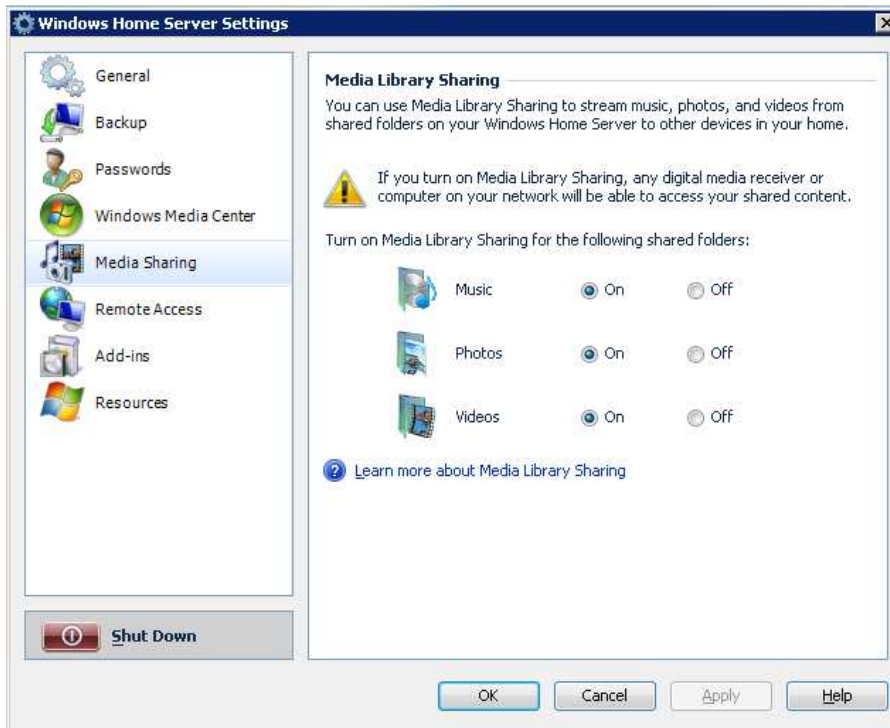
ClamWin on vapaaseen lähdekoodiin perustuva virustorjuntaohjelmisto, joka tunnistaa useimmat virus- ja haittaohjelmatyypit. Ainoa huono puoli on tosiaikaisen skannauksen puuttuminen, joten käyttäjän on aikataulettava itse milloin virustarkistuksia ajetaan. ClamWin löytyy osoitteesta <http://www.clamwin.com>.

6.1.10 Median streamaus (Media Streaming/Media Sharing)

Windows Home Server voi toimia myös median streamaus -palvelimena. Kotiverkossa voi olla monia laitteita, jotka hyötyvät tästä ominaisuudesta, kuten esimerkiksi pelikonsolit, mediasoittimet ja tietokoneet. Lyhyesti sanottuna median streamaus mahdollistaa musiikki-, kuva- ja videotiedostojen jakamisen

palvelimelta toisiin kotiverkon laitteisiin. Laitteet voivat sijaita eri huoneissa, joten esimerkiksi elokuvan katsominen on mahdollista vaikka makuuhuoneessa sijaitsevalla tietokoneella tai pelikonsolilla, joka on kytketty palvelimeen. Streamaus-palvelu asetetaan päälle seuraavanlaisesti:

1. Painetaan konsolista löytyvää Settings-painiketta ja valitaan Media Sharing –välilehti (Kuvio 20).



KUVIO 20. Media Sharing

2. Asetetaan kaikki vaihtoehdot On-asentoon.
3. Painetaan OK.

Tämän jälkeen jaettua mediaa voidaan toistaa/streamata esimerkiksi PC:ssä Windows Media Player 12 ja Windows Media Center –ohjelmilla. Mikäli streamausta halutaan erillisiin mediavastaanottimiin tai pelikonsoleihin, on niissä oltava tuki joko WMC:lle (Windows Media Connect, MCX:lle (Media Center Extender) tai DLNA:lle (The Digital Living Network Alliance). Testien aikana huomattiin, että elokuvien streamaus tökki pahasti langattomalla g-

luokan nopeudella kannettavaan tietokoneeseen käyttäen Windows Media Center –ohjelmistoa. Langallisella yhteydellä pöytäkoneeseen streamaus toimi kuitenkin hyvin.

6.2 Amahi Home Server

Samalla tavalla kuin Windows Home Serveriin myös Amahiin tehdään tarvittavat konfiguroinnit asennuksen jälkeen, jotta se saadaan kunnan toimintakuntoon. Tarkistetaan toimiiko Ethernet-yhteys oikein eli mikäli verkkolaitteet ja kaapelointi ovat kunnossa, porttivalon pitäisi palaa kiinteästi joko kytkimessä, reitittimessä tai modeemissa, riippuen mihin näistä palvelin on kytketty.

Windows Home Serverissä asiakaskoneet piti yhdistää palvelimeen erillisellä ohjelmistolla. Amahi Home Serverissä lähiverkon asiakaskoneet yhdistetään automaattisesti palvelimeen, joten mitään erillisiä ohjelmistoja ei tarvitse ajaa.

Amahia hallitaan selaimen kautta Amahi Dashboardissa (Kuvio 21), jonne päästään palvelimelta tai asiakaskoneelta syöttämällä selaimen osoiteriville hda ja kirjautumalla sisään Fedoran tunnuksilla.

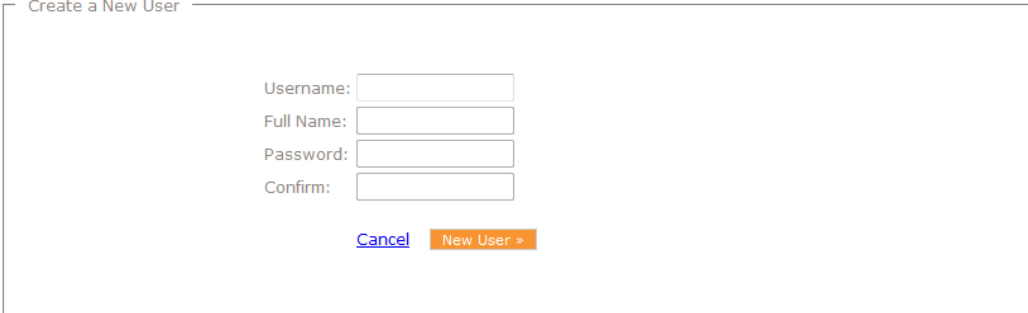


KUVIO 21. Amahin hallintapaneeli (The Dashboard)

6.2.1 Käyttäjien luominen (Users)

Ensimmäiseksi tulee luoda käyttäjät. Mennään aiemmin mainittujen ohjeiden mukaisesti Amahin hallintapaneeliin ja suoraan asetuksiin kirjoittamalla selaimen osoiteriville <http://setup>. Käyttäjä lisätään seuraavasti:

1. Mennään Users-välilehdelle. Listassa pitäisi näkyä jo yksi käyttäjä, joka on luotu aiemmin Fedoran asennuksen aikana.
2. Painetaan New User.
3. Syötetään käyttäjätiedot (Kuvio 22) ja painetaan vielä New User –painiketta.



Create a New User

Username:

Full Name:

Password:

Confirm:

[Cancel](#) [New User >](#)

Kuvio 22 Käyttäjän luominen

6.2.2 Jakokansioiden luominen (Shares)

Edellisen vaiheen jälkeen voidaan luoda käyttäjille uusia kansioita. Kansioita lisätään ja muokataan seuraavanlaisesti:

1. Menemällä Shares-välilehdelle eteen tulee lista palvelimella olevista jakokansioista.
2. Painamalla New Share voidaan luoda uusi jakokansio (Kuvio 23).

Create a New Share

Name:

Path:

Visible:

Read Only:

[Cancel](#) [Create this Share >](#)

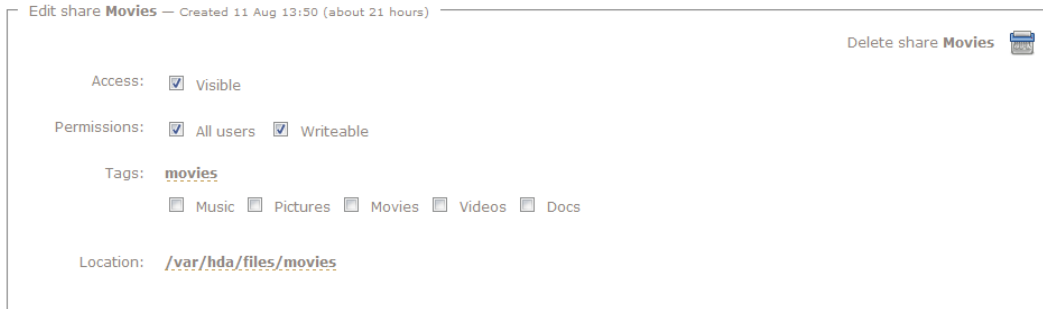
KUVIO 23. Jakokansion lisääminen

3. Syötetään jakonimi.
4. Path Name kuvastaa minne tiedostot varsinaisesti tallennetaan mutta sitä ei tarvitse määrittää itsellä.
5. Visible-valinnalla voidaan määrittää kansio näkyväksi tai piilotetuksi käyttäjiltä.
6. Read Only voidaan ruksata, mikäli kansioon halutaan pelkät lukuoikeudet.
7. Painetaan Create This Share, jonka jälkeen kansion pitäisi näkyä Shares-välilehdellä.

6.2.3 Jakokansioiden muokkaaminen (Shares)

Shares-välilehdeltä voidaan hallita jo valmiina olevia jakokansioita, jotka ovat Books, Docs, Movies, Music sekä Pictures:

1. Painetaan jakokansiota, mitä halutaan muokata Shares-välilehdellä, jolloin eteen tulee Edit share -ruutu (Kuvio 24).

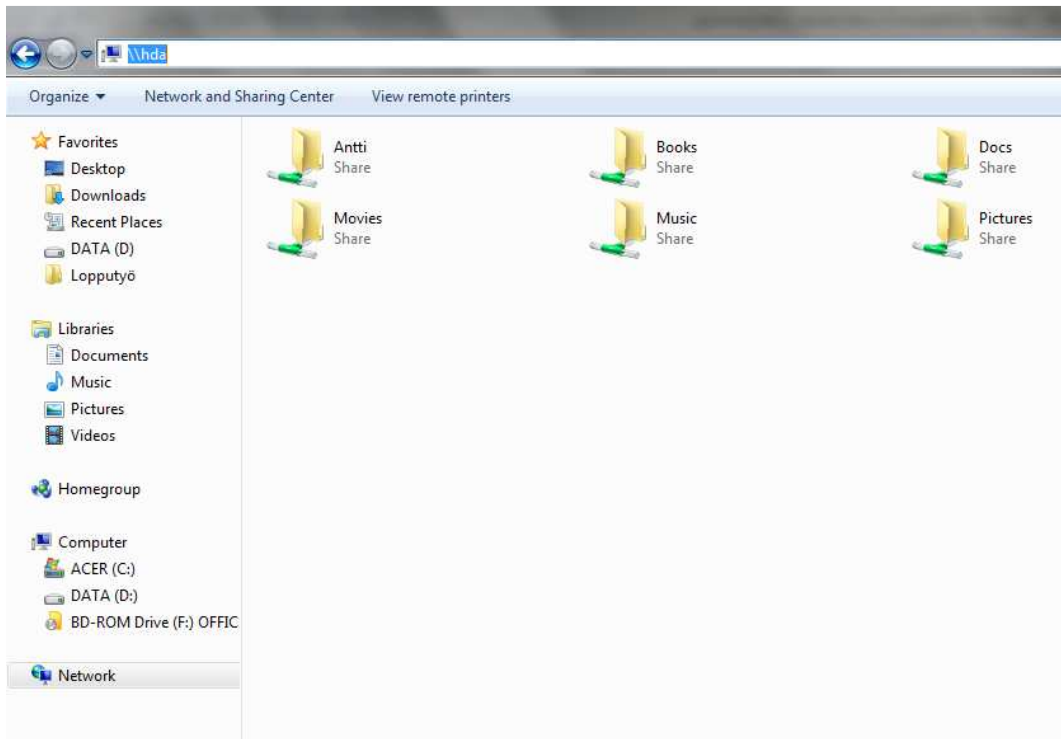


KUVIO 24. Jakokansion oikeudet

2. Visible tarkoittaa, että jakokansio näkyy suoraan käyttäjille.
3. Oletuksena oikeudet jakokansioihin ovat kaikille käyttäjille mutta ruksaamalla pois All users –valinnan, voidaan määritellä vain tietyille käyttäjille oikeudet kansioon. Kannattaa huomioida, että jos All users –valinta on päällä, tulee kaikille uusille käyttäjille automaattisesti täydet oikeudet kansioon.
4. Valitaan Access niille käyttäjille, joille halutaan antaa oikeus päästä kansioon ja Write niille, joille halutaan kirjoitusoikeudet.

6.2.4 Jakokansioiden käyttäminen

Palvelimen jakokansioihin päästään käsiksi lähiverkon kautta polusta \\hda. Syöttämällä esimerkiksi Windowsin Resurssienhallinnan osoiteriville \\hda päästään palvelimen jakokansioihin (Kuvio 25). Jos jakokansioiden käyttäjillä on samat tunnukset ja salasanat kuin Windowsissa pitäisi kansioihin päästä suoraan.



KUVIO 25. Jakokansiot

6.2.5 Ohjelmien asentaminen (Apps)

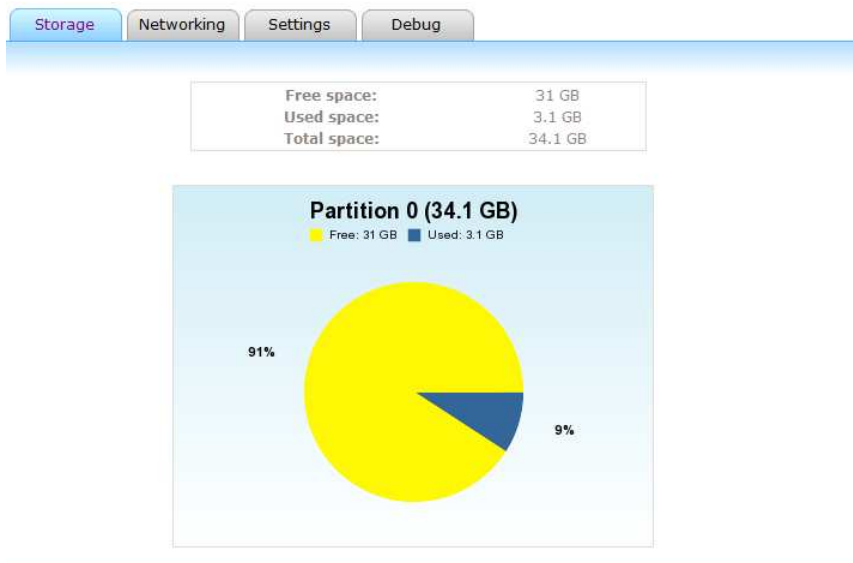
Palvelimessa ei ole oletuksena kovin paljoa toiminnallisuuksia. Niitä voidaan kuitenkin laajentaa nopeasti ja näppärästi. Apps-välilehdeltä saa näkyviin listan saatavilla olevista ohjelmista painamalla Available-painiketta (Kuvio 26). Kun listassa näkyvän ohjelman nimeä painetaan, laajenee eteen tarkempi kuvaus ohjelmasta ja Install-painike, josta ohjelma voidaan asentaa.



KUVIO 26. Lista asennettavista ohjelmista

6.2.6 Osiot ja levyt (Storage)

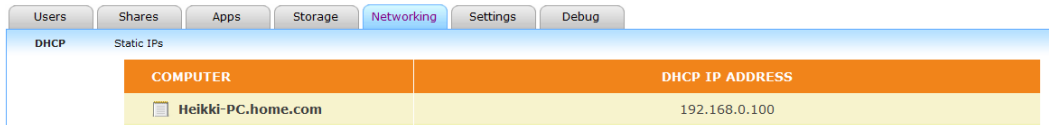
Storage-välilehdeltä (Kuvio 27) saadaan näkyviin osioiden ja levyjen tietoja. Partitions-osassa näkyy aktiivisten osioiden tilajakauma eli yhteinen, vapaa sekä käytössä oleva tilamäärä. Disks-kohtasta näkyviin tulee levyjen tietoja, kuten malli ja fyysinen polku sekä lämpötilatiedot.



KUVIO 27. Tilajakauma

6.2.7 Verkkohallinta (Networking)

Verkkohallinnasta löytyy DHCP-lista asiakaskoneista (Kuvio 27), jotka ovat kiinni palvelimessa. Asiakaskoneista näkyy nimi ja IP-osoite. Static IPs -kohdasta voidaan halutessaan lisätä uusi staattinen IP-osoite kotiverkon koneille.

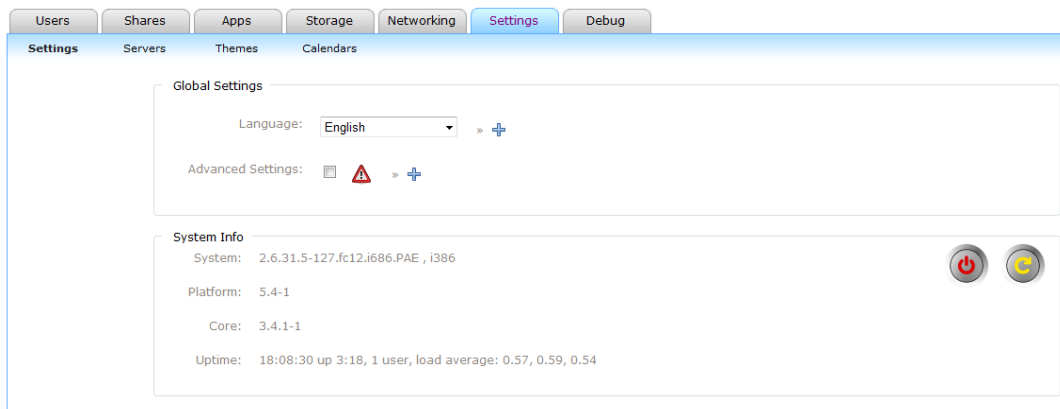


COMPUTER	DHCP IP ADDRESS
<input type="checkbox"/> Heikki-PC.home.com	192.168.0.100

KUVIO 28. DHCP-lista

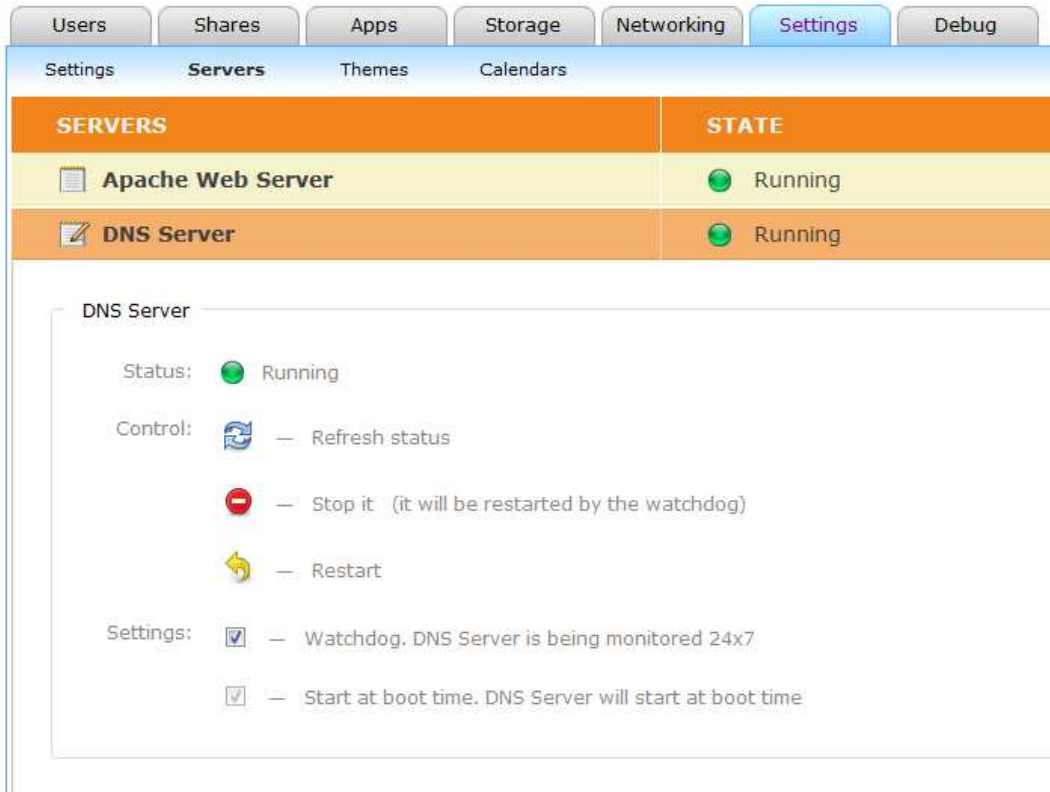
6.2.8 Asetukset (Settings)

Palvelimeen liittyviä järjestelmäasetuksia päästään muuttamaan Settings-välilehdeltä (Kuvio 29), joka näyttää lisäksi tietoa järjestelmän versioista ja kuinka pitkään palvelin on ollut päällä. Palvelin voidaan myös sammuttaa ja käynnistää uudestaan.



KUVIO 29. Järjestelmäasetukset

Servers-kohdasta nähdään lista palvelimessa olevista palveluista (Kuvio 30). Palveluita voidaan sammuttaa ja käynnistää uudelleen sekä määrittää esimerkiksi käynnistymään palvelimen käynnistyksen yhteydessä.



KUVIO 30. Palvelut

Lisäksi voidaan vaihtaa Dashboardin ulkoasuja Themes-kohdasta, mikäli niitä on asennettu palvelimeen. Calendars-kohdasta voidaan määrittellä kalentereita esimerkiksi Outlook-ohjelmaa varten.

6.2.9 Palvelimen lokitiedot (Debug)

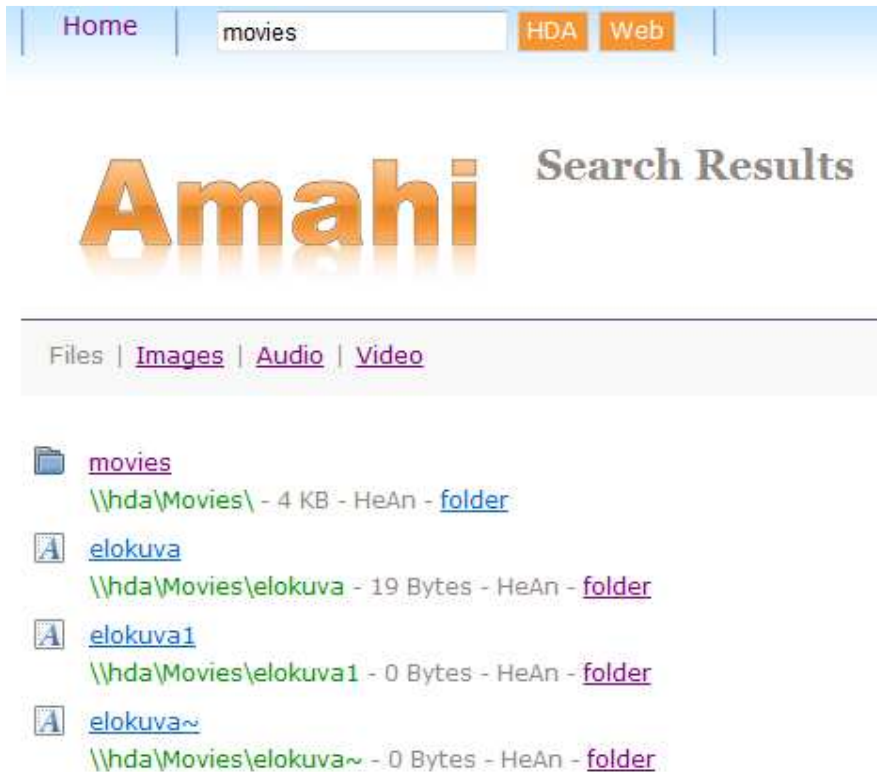
Palvelimen toimintaa voidaan seurata tarkemmin lokitiedoista, jotka löytyvät Debug-välilehdeltä (Kuvio 31). Virhetilanteen sattuessa lokitiedoista voi olla suuri apu, koska niiden avulla virheen alkuperä ja sijainti voidaan jäljittää nopeammin ja tehokkaammin. Debug näyttää myös muuta hyödyllistä tietoa, kuten esimerkiksi prosessoritiedot, muistin käyttöä koskevat tiedot sekä kuormitustiedot.

Users	Shares	Apps	Storage	Networking	Settings	Debug																																																																																							
<table border="1"> <thead> <tr> <th>App Logs</th> <th>System</th> <th>Logs</th> </tr> </thead> <tbody> <tr> <td colspan="3">18:24:20 up 3:34, 1 user, load average: 0.00, 0.05, 0.24</td> </tr> <tr> <td colspan="3">processor: 0</td> </tr> <tr> <td colspan="3">vendor_id: AuthenticAMD</td> </tr> <tr> <td colspan="3">cpu family : 6</td> </tr> <tr> <td colspan="3">model : 8</td> </tr> <tr> <td colspan="3">model name : AMD Sempron(tm) 2600+</td> </tr> <tr> <td colspan="3">stepping : 1</td> </tr> <tr> <td colspan="3">cpu MHz : 1835.534</td> </tr> <tr> <td colspan="3">cache size : 256 KB</td> </tr> <tr> <td colspan="3">fdiv_bug : no</td> </tr> <tr> <td colspan="3">hlt_bug : no</td> </tr> <tr> <td colspan="3">f00f_bug : no</td> </tr> <tr> <td colspan="3">coma_bug : no</td> </tr> <tr> <td colspan="3">fpu : yes</td> </tr> <tr> <td colspan="3">fpu_exception : yes</td> </tr> <tr> <td colspan="3">cpuid level : 1</td> </tr> <tr> <td colspan="3">wp : yes</td> </tr> <tr> <td colspan="3">flags : fpu vme de pse tsc msr pae mce cx8 apic mtrr pge mca cmov pat pse36 mmx fxsr sse</td> </tr> <tr> <td colspan="3">bogomips : 3671.06</td> </tr> <tr> <td colspan="3">clflush size : 32</td> </tr> <tr> <td colspan="3">power management: ts</td> </tr> <tr> <td colspan="3">MemTotal: 1253688 kB</td> </tr> <tr> <td colspan="3">MemFree: 418236 kB</td> </tr> <tr> <td colspan="3">Buffers: 146016 kB</td> </tr> <tr> <td colspan="3">Cached: 352288 kB</td> </tr> <tr> <td colspan="3">SwapCached: 0 kB</td> </tr> <tr> <td colspan="3">Active: 487836 kB</td> </tr> <tr> <td colspan="3">-----</td> </tr> </tbody> </table>							App Logs	System	Logs	18:24:20 up 3:34, 1 user, load average: 0.00, 0.05, 0.24			processor: 0			vendor_id: AuthenticAMD			cpu family : 6			model : 8			model name : AMD Sempron(tm) 2600+			stepping : 1			cpu MHz : 1835.534			cache size : 256 KB			fdiv_bug : no			hlt_bug : no			f00f_bug : no			coma_bug : no			fpu : yes			fpu_exception : yes			cpuid level : 1			wp : yes			flags : fpu vme de pse tsc msr pae mce cx8 apic mtrr pge mca cmov pat pse36 mmx fxsr sse			bogomips : 3671.06			clflush size : 32			power management: ts			MemTotal: 1253688 kB			MemFree: 418236 kB			Buffers: 146016 kB			Cached: 352288 kB			SwapCached: 0 kB			Active: 487836 kB			-----		
App Logs	System	Logs																																																																																											
18:24:20 up 3:34, 1 user, load average: 0.00, 0.05, 0.24																																																																																													
processor: 0																																																																																													
vendor_id: AuthenticAMD																																																																																													
cpu family : 6																																																																																													
model : 8																																																																																													
model name : AMD Sempron(tm) 2600+																																																																																													
stepping : 1																																																																																													
cpu MHz : 1835.534																																																																																													
cache size : 256 KB																																																																																													
fdiv_bug : no																																																																																													
hlt_bug : no																																																																																													
f00f_bug : no																																																																																													
coma_bug : no																																																																																													
fpu : yes																																																																																													
fpu_exception : yes																																																																																													
cpuid level : 1																																																																																													
wp : yes																																																																																													
flags : fpu vme de pse tsc msr pae mce cx8 apic mtrr pge mca cmov pat pse36 mmx fxsr sse																																																																																													
bogomips : 3671.06																																																																																													
clflush size : 32																																																																																													
power management: ts																																																																																													
MemTotal: 1253688 kB																																																																																													
MemFree: 418236 kB																																																																																													
Buffers: 146016 kB																																																																																													
Cached: 352288 kB																																																																																													
SwapCached: 0 kB																																																																																													
Active: 487836 kB																																																																																													

KUVIO 31. Debug

6.2.10 Hakutoiminto (Search HDA/Web)

Amahin hallintapaneelin vasemmasta yläreunasta löytyy hakutoiminto (Kuvio 32), jolla voidaan etsiä esimerkiksi tiedostoja palvelimelta tai käyttää sitä normaalina hakutoimintona Internet-sivuja varten. Hakutoiminnon käytettävyys on kuitenkin vielä hiukan huono, koska haku ei löydä tuoreeltaan lisättyjä tiedostoja palvelimeen ennen kuin järjestelmään on ajettu updatedb-komento Fedoran komentokehotteessa.



KUVIO 32. Hakutoiminto

6.2.11 Varmuuskopioiden tekeminen

Mikäli asiakaskoneissa on esimerkiksi Windows Vista tai 7 onnistuu varmuuskopioiden tekeminen melko helposti Amahi Home Serveriin. Ensin kannattaa luoda palvelimeen oma kansio varmuuskopiointia esimerkiksi käyttäjäkansioon. Tämän jälkeen mennään Windowsissa Varmuuskopioi ja palauta -ohjelmaan (Backup & Restore Center), joka löytyy ohjauspaneelistä (Control Panel).

1. Painetaan määritä varmuuskopiointi.
2. Painetaan Tallenna verkkoon painiketta ja laitetaan verkkosijainniksi \\hda\omakansio\backups. Tämän jälkeen syötetään vielä verkon tunnistetiedot joita Windowsin varmuuskopiointi tarvitsee verkkokopiointia varten.

3. Valitaan listalta lisätty verkkosijainti uudestaan ja painetaan seuraava.
4. Valitaan halutaanko Windowsin määrittää varmuuskopiotavat tiedostot tai itse määritetään. Painetaan Seuraava.
5. Valitaan mitä halutaan varmuuskopioida
6. Painetaan Tallenna asetukset ja suorita varmuuskopiointi.

6.2.12 Streamaus Amahissa

Myös Amahi Home Serverin voi valjastaa streamaus-palvelimeksi. Tämä onnistuu asentamalla DLNA:n Apps-osiosta. Tätä ennen tulee olla asennettuna RPM Fusion (Free) ja RPM Fusion (Non-Free) ohjelmat, jotka löytyvät myös Apps-osiosta.

Amahista on mahdollista streamata esimerkiksi PC:hen Windows Media Player 12 ja Windows Media Center -ohjelmilla. Mikäli streamausta halutaan erillisiin mediavastaanottimiin tai pelikonsoleihin, on niissä oltava tuki DLNA:lle. Testien aikana huomattiin, että toisin kuin Windows Home Serverissä elokuvien streamaus toimi loistavasti langattomalla g-luokan nopeudella kannettavaan tietokoneeseen Windows Media Centerillä. Myös langallisella yhteydellä streamaus pöytäkoneeseen toimi ongelmitta.

6.3 Reitittimen konfigurointi

Jos lähiverkkosi käyttää reititintä, yhdyskäytävää tai muuta rautapohjaista palomuuria täytyy siihen määrittää oikeanlaiset porttiasetukset. Porttiasetukset löytyvät yleensä reitittimien Port Forwarding –osiosta (Kuvio 33), johon täytyy laittaa seuraavanmukaiset asetukset:

Portti 80 (HTTP), käyttäen TCP-protokollaa. (Windows Home Server)

Portti 443 (SSL), käyttäen TCP-protokollaa. (Windows Home Server)

Portti 4125 (RDP), käyttäen TCP-protokollaa. (Windows Home Server)

Portti 1194 (VPN), käyttäen UDP-protokollaa. (Amahi Home Server)

Product Page : DIR-600 Hardware Version : Bx Firmware Version : 2.02

D-Link

DIR-600 // SETUP ADVANCED MAINTENANCE STATUS HELP

Port Forwarding

ADVANCED PORT FORWARDING RULES

The Advanced Port Forwarding option allows you to define a single public port on your router for redirection to an internal LAN IP Address and Private LAN port if required. This feature is useful for hosting online services such as FTP or Web Servers.

Save Settings Don't Save Settings

24 - ADVANCED PORT FORWARDING RULES

Remaining number of rules that can be created: 21

			Port	Traffic Type
<input checked="" type="checkbox"/>	Name WHS Remote	<<< Application Name	Public Port 80 ~ 80	TCP
	IP Address 192.168.0.100	<<< Computer Name	Private Port 80 ~ 80	
<input checked="" type="checkbox"/>	Name WHS Remote	<<< Application Name	Public Port 443 ~ 443	TCP
	IP Address 192.168.0.100	<<< Computer Name	Private Port 443 ~ 443	
<input checked="" type="checkbox"/>	Name WHS Remote	<<< Application Name	Public Port 4125 ~ 4125	Any
	IP Address 192.168.0.100	<<< Computer Name	Private Port 4125 ~ 4125	

Helpful Hints..

- Check the **Application Name** drop-down menu for a list of pre-defined applications that you can select from. If you select one of the pre-defined applications, click the arrow button next to the drop-down menu to fill out the appropriate fields.
- You can select your computer from the list of DHCP clients in the **Computer Name** drop-down menu, or enter the IP address manually of the computer you would like to open the specified port to.
- This feature allows you to open a range of ports to a computer on your network. To do so, enter the first port in the range you would like to open on the router in the first box under **Public Port** and last port of the range in the second one. After that you enter the first port in the range that the internal server uses in the first box under **Private Port** and the last port of the range in the second.
- To open a single port using this feature, simply enter the same number in both boxes.

KUVIO 33. Esimerkki D-Linkin reitittimen porttiasetuksista

Mikäli porttiasetuksia ei määritetä, reititin tai muu laite ei osaa reitittää Internetistä päin tulevia pyyntöjä, jotka kohdistuvat palvelimeen. Tällöin esimerkiksi Remote Access –palvelu ei toimi eikä myöskään palvelimen sivusto.

7 TIEDONSIIRTONOPEUDET

Testasimme palvelimen molempien järjestelmien tiedonsiirtonopeuksia lähiverkon kautta langallisesti ja langattomasti pöytäkoneesta sekä kannettavasta tietokoneesta. Laitteiden välissä oleva reititin on N-luokan D-Link DIR-600. Seuraavassa palvelimen (Kuvio 34), pöytäkoneen (Kuvio 35) sekä kannettavan (Kuvio 36) speksit.

KUVIO 14. Palvelinkone

Emolevy	Acer G74M
Proessori	AMD Sempron 2600+
Muisti	1,3 Gt DDR-200
Kiintolevy	WDC WD800BB 80 GB
Verkko	Fast Ethernet (RJ45)
Käyttöjärjestelmä	Windows Home Server / Amahi Home Server (Fedora 12)

KUVIO 35. Pöytäkone

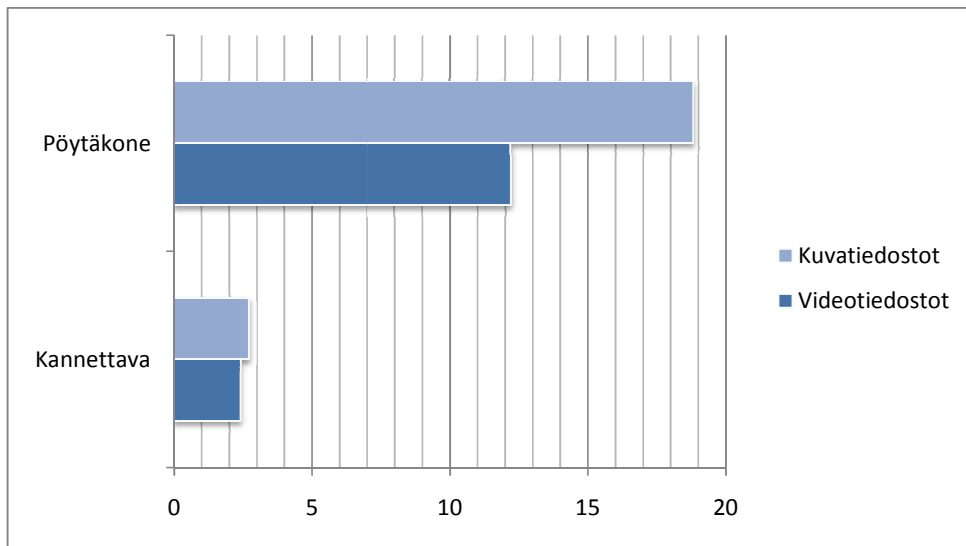
Emolevy	MSI MS-7238
Proessori	Intel Core 2 Duo E6400
Muisti	2 Gt Kingston KTC1G DDR2-400
Kiintolevy	Samsung HD103SJ 1 Tt SATA
Verkko	Gigabit Ethernet (RJ45)
Käyttöjärjestelmä	Windows 7 Professional

KUVIO 36. Kannettava

Emolevy	Acer TravelMate 7520
Proessori	AMD Turion64 X2 TL-60
Muisti	3 Gt Hyundai DDR-333
Kiintolevy	WDC WD2500BEVS 250 GB
Verkko	Broadcom 802.11g 54 Mbps
Käyttöjärjestelmä	Windows 7 Home Premium

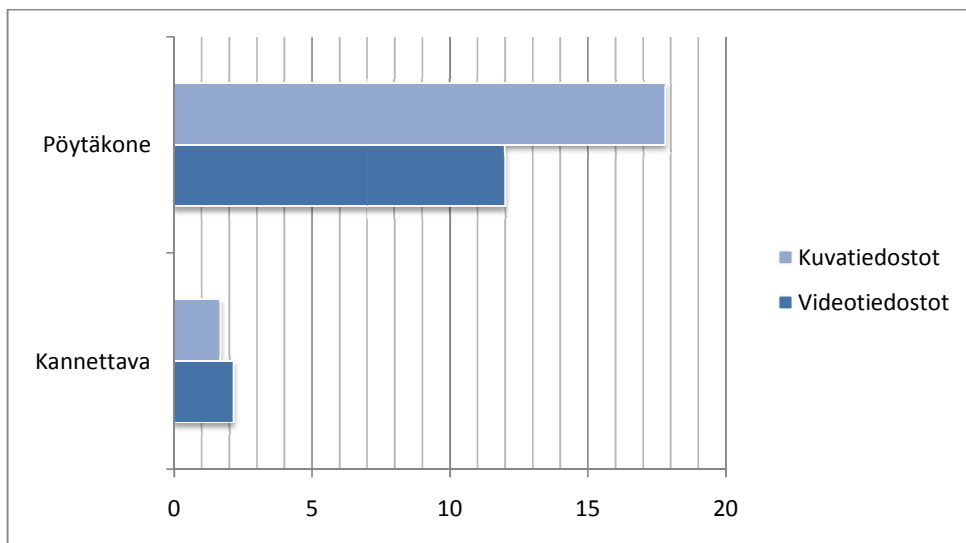
Windows Home Serverissä palvelimelta pöytäkoneelle langallisella yhteydellä isot videotiedostot (600-800Mb) siirtyivät noin 12,2Mb/s ja joukko kuvatiedostoja (100-1000Kb) noin 18,8Mb/s. Kannettavaan langattomalla yhteydellä isot videotiedostot siirtyivät noin 2,4Mb/s ja kuvatiedostot 2,4-3,0Mb/s (Kuvio 37).

KUVIO 37. Tiedonsiirtonopeustulokset Windows Home Serverissä



Amahi Home Serverissä tiedostonsiirtonopeudet vaihtelivat jonkin verran. Palvelimelta pöytäkoneelle langallisella yhteydellä isot videotiedostot (600-800Mb) siirtyivät noin 11-13Mb/s ja joukko kuvatiedostoja (100-1000Kb) noin 17,8Mb/s. Kannettavaan langattomalla yhteydellä isot videotiedostot siirtyivät noin 1,9-2,4Mb/s ja kuvatiedostot 1,5-1,8Mb/s (Kuvio 38).

KUVIO 38. Tiedonsiirtonopeustulokset Amahi Home Serverissä



8 TIETOTURVATESTIT

Suoritimme molempiin kotipalvelinjärjestelmiin tietoturvatestejä käyttäen Nessus-tietoturvakannetta. Lyhyesti sanottuna Nessus suorittaa porttiskannauksia sekä erilaisia haavoittuvuustestejä kohdejärjestelmään. Porttiskannaus selvittää kohdejärjestelmän aktiivisena olevat portit (TCP tai UDP). Esimerkiksi Windows Home Serverissä on aktiivinen TCP-portti 80 HTTP liikennettä varten, joka konfiguroitiin myös reitittimeen.

Ennen skannauksen aloittamista valitaan mitä haavoittuvuuksia kohdejärjestelmästä halutaan testata eli valitaan pluginit, joita käytetään. Nessuksessa kannattaa olla päällä valinta Safe Checks, sillä se estää vaarallisten pluginien ajamisen, jotka voivat pahimmassa tapauksessa rikkoa kohdejärjestelmän. Plugineja on oletuksena valittu melko paljon, joten halutessaan voi harkita mitä plugineja kannattaa jättää pois. Toisaalta voidaan ajaa kaikki ei-vaarallisetkin testit, sillä jos jotain pluginin kohdetta ei löydy, ei testiä ajeta sille ollenkaan.

Testit ajettiin molempiin järjestelmiin kaikilla ei-vaarallisilla plugineilla. Nessus löysi Windows Home Serveristä kolmekymmentäkaksi (32) matalan tason (low) riskiä ja kolme (3) keskitason (medium) riskiä. Amahi Home Serveristä löytyi kaksikymmentäseitsemän (27) matalan tason (low) ja neljä (4) keskitason (medium) riskiä. Matalan tason riskit olivat melko yleisiä, joilla saatiin esimerkiksi selville, minkälainen käyttöjärjestelmä kohdejärjestelmässä on, tietoa käytössä olevasta HTTP-protokollasta sekä aikavyöhyketietoja.

Windows Home Serveristä löytyi haavoittuvuus, joka sallii heikkojen salausten käyttämisen isäntäkoneessa, jotka tarjoavat pelkästään heikon salauksen tai ei salausta ollenkaan (Kuvio 39).

Plugin ID: 26928

Port / Service: www (443/tcp)

Plugin Name: SSL Weak Cipher Suites Supported

Synopsis

The remote service supports the use of weak SSL ciphers.

Description

The remote host supports the use of SSL ciphers that offer either weak encryption or no encryption at all.

Solution

Reconfigure the affected application if possible to avoid use of weak ciphers.

See Also

<http://www.openssl.org/docs/apps/ciphers.html>

CVSS

5.0 (CVSS2#AV:N/AC:L/Au:N/C:P/I:N/A:N)

Plugin Output

Here is the list of weak SSL ciphers supported by the remote server :

Low Strength Ciphers (< 56-bit key)

SSLv2

EXP-RC2-CBC-MD5	Kx=RSA(512)	Au=RSA	Enc=RC2(40)	Mac=MD5	export
EXP-RC4-MD5	Kx=RSA(512)	Au=RSA	Enc=RC4(40)	Mac=MD5	export

SSLv3

EXP-RC2-CBC-MD5	Kx=RSA(512)	Au=RSA	Enc=RC2(40)	Mac=MD5	export
EXP-RC4-MD5	Kx=RSA(512)	Au=RSA	Enc=RC4(40)	Mac=MD5	export

The fields above are :

{OpenSSL ciphername}

Kx={key exchange}

Au={authentication}

Enc={symmetric encryption method}

Mac={message authentication code}

{export flag}

KUVIO 39. SSL Weak Cipher Suites

Toinen haavoittuvuus sallii keskivahvan salausten käyttämisen isäntäkoneessa. Keskivahvassa salauksessa pituuden tulisi olla vähintään 56 bittiä ja vähemmän kuin 112 bittiä (Kuvio 40).

Plugin ID: 42873

Port / Service: www (443/tcp)

Plugin Name: SSL Medium Strength Cipher Suites Supported

Synopsis

The remote service supports the use of medium strength SSL ciphers.

Description

The remote host supports the use of SSL ciphers that offer medium strength encryption, which we currently regard as those with key lengths at least 56 bits and less than 112 bits.

Solution

Reconfigure the affected application if possible to avoid use of medium strength ciphers.

CVSS

5.0 (CVSS2#AV:N/AC:L/Au:N/C:P/I:N/A:N)

Plugin Output

Here are the medium strength SSL ciphers supported by the remote server :

Medium Strength Ciphers (>= 56-bit and < 112-bit key)

SSLv2

DES-CBC-MD5 Kx=RSA Au=RSA Enc=DES(56) Mac=MD5

SSLv3

DES-CBC-SHA Kx=RSA Au=RSA Enc=DES(56) Mac=SHA1

The fields above are :

{OpenSSL ciphername}

Kx={key exchange}

Au={authentication}

Enc={symmetric encryption method}

Mac={message authentication code}

{export flag}

KUVIO 40. SSL Medium Strength Cipher Suites

Kolmas haavoittuvuus mahdollistaa hyökkääjään pääsemään käsiksi isäntäkoneeseen käyttäen Remote Desktop -protokollaa. Se on haavoittuvainen MiTM (Man in the Middle) hyökkäyksille (Kuvio 41).

Plugin ID: 18405

Port / Service: msrdp (3389/tcp)

Plugin Name: Microsoft Windows Remote Desktop Protocol Server Man in the Middle Weakness

Synopsis

It may be possible to get access to the remote host.

Description

The remote version of the Remote Desktop Protocol Server (Terminal Service) is vulnerable to a man in the middle (MiTM) attack. The RDP client makes no effort to validate the identity of the server when setting up encryption. An attacker with the ability to intercept traffic from the RDP server can establish encryption with the client and server without being detected. A MiTM attack of this nature would allow the attacker to obtain any sensitive information transmitted, including authentication credentials.

This flaw exists because the RDP server stores a hardcoded RSA private key in the mstlsapi.dll library. Any local user with access to this file (on any Windows system) can retrieve the key and use it for this attack.

Solution

Force the use of SSL as a transport layer for this service.

See Also

<http://www.oxid.it/downloads/rdp-gbu.pdf>
<http://technet.microsoft.com/en-us/library/cc782610.aspx>

CVSS

5.1 (CVSS2#AV:N/AC:H/Au:N/C:P/I:P/A:P)

CVE

CVE-2005-1794

BID

13818

Xref

OSVDB:17131

KUVIO 41. Man in the Middle Weakness

Esittelemme lisäksi tarkempia esimerkkejä keskitason riskeistä Amahi Home Serverissä. Yksi riskeistä (Kuvio 42) salli hyökkääjän tehdä listan lähiverkossa sijaitsevista potentiaalisista kohteista käyttäen hyväksi DNS Zone Transferia.

Plugin ID: 10595 **Port / Service:** dns (53/tcp)

Plugin Name: DNS Server Zone Transfer Information Disclosure (AXFR)

Synopsis
The remote name server allows zone transfers

Description
The remote name server allows DNS zone transfers to be performed.

A zone transfer lets a remote attacker instantly populate a list of potential targets. In addition, companies often use a naming convention that can give hints as to a servers primary application (for instance, proxy.example.com, payroll.example.com, b2b.example.com, etc.).

As such, this information is of great use to an attacker, who may use it to gain information about the topology of the network and spot new targets.

Solution
Limit DNS zone transfers to only the servers that need the information.

See Also
<http://en.wikipedia.org/wiki/AXFR>

CVSS
5.0 (CVSS2#AV:N/AC:L/Au:N/C:P/I:N/A:N)

CVE
CVE-1999-0532

Xref
OSVDB:492

KUVIO 42. DNS Zone Transfer

Toisena riskinä (Kuvio 43) oli DNS-palvelimen haavoittuvuus urkkimiselle. Tämän avulla hyökkääjä voi selvittää tietoja esimerkiksi käyttäjien Internet-selailuista ja ulkoisista sähköpostipalvelimista.

Plugin ID: 12217

Port / Service: dns (53/udp)

Plugin Name: DNS Server Cache Snooping Remote Information Disclosure

Synopsis

The remote DNS server is vulnerable to cache snooping attacks.

Description

The remote DNS server responds to queries for third-party domains that do not have the recursion bit set.

This may allow a remote attacker to determine which domains have recently been resolved via this name server, and therefore which hosts have been recently visited.

For instance, if an attacker was interested in whether your company utilizes the online services of a particular financial institution, they would be able to use this attack to build a statistical model regarding company usage of that financial institution. Of course, the attack can also be used to find B2B partners, web-surfing patterns, external mail servers, and more.

Note: If this is an internal DNS server not accessible to outside networks, attacks would be limited to the internal network. This may include employees, consultants and potentially users on a guest network or WiFi connection if supported.

Solution

Use another DNS software.

See Also

For a much more detailed discussion of the potential risks of allowing DNS cache information to be queried anonymously, please see: http://www.rootsecure.net/content/downloads/pdf/dns_cache_snooping.pdf

CVSS

5.0 (CVSS2#AV:N/AC:L/Au:N/C:P/I:N/A:N)

KUVIO 43. DNS Server Cache Snooping

Kolmas riski (Kuvio 44) voi sallia hyökkäjän käyttää web-palvelimessa TRACE ja TRACK –metodeja. Niillä voidaan selvittää esimerkiksi minne web-palvelin on yhteydessä.

Plugin ID: 11213 **Port / Service:** http? (80/tcp)

Plugin Name: HTTP TRACE / TRACK Methods Allowed

Synopsis
Debugging functions are enabled on the remote web server.

Description
The remote webserver supports the TRACE and/or TRACK methods. TRACE and TRACK are HTTP methods that are used to debug web server connections.

Solution
Disable these methods. Refer to the plugin output for more information.

See Also
http://www.cgisecurity.com/whitehat-mirror/WH-WhitePaper_XST_ebook.pdf
<http://www.apacheweek.com/issues/03-01-24>
<http://www.kb.cert.org/vuls/id/288308>
<http://www.kb.cert.org/vuls/id/867593>
<http://sunsolve.sun.com/search/document.do?assetkey=1-66-200942-1>

CVSS
4.3 (CVSS2#AV:N/AC:M/Au:N/C:P/I:N/A:N)

Plugin Output
To disable these methods, add the following lines for each virtual host in your configuration file :

```
RewriteEngine on
RewriteCond %{REQUEST_METHOD} ^(TRACE|TRACK)
RewriteRule .* - [F]
```

Alternatively, note that Apache versions 1.3.34, 2.0.55, and 2.2 support disabling the TRACE method natively via the 'TraceEnable' directive.

Nessus sent the following TRACE request :

```
----- snip -----
TRACE /Nessus1449517550.html HTTP/1.1
Connection: Close
Host: hda.home.com
Pragma: no-cache
```

KUVIO 44. TRACE ja TRACK –metodit

Neljäs riski (Kuvio 45) mahdollistaa kenen tahansa selvittää etäkohteen tietoja, kuten käyttöjärjestelmän tyyppin ja version, isännänimen ja käytössä olevat palvelut. Amahista testi löysi tietokoneen nimen, MAC-osoitteen ja käyttöjärjestelmätyypin.

Plugin ID: 12218 **Port / Service:** mdns (5353/udp)
Plugin Name: mDNS Detection

Synopsis
It is possible to obtain information about the remote host.

Description
The remote service understands the Bonjour (also known as ZeroConf or mDNS) protocol, which allows anyone to uncover information from the remote host such as its operating system type and exact version, its hostname, and the list of services it is running.

Solution
Filter incoming traffic to UDP port 5353 if desired.

CVSS
5.0 (CVSS2#AV:N/AC:L/Au:N/C:P/I:N/A:N)

Plugin Output
Nessus was able to extract the following information :

- Computer name : kotipalvelin.local.
- Ethernet addr : 00:0f:ea:a2:c0:8b
- Computer Type : i686
- Operating System : LINUX

KUVIO 45. mDSN Detection

Raporteissa näkyvät teknillisesti mutta selkeästi testien kuvaukset (Description) ja tulokset (Plugin Output) sekä useissa tapauksissa myös ratkaisut (Solution), joilla haavoittuvuudet voidaan paikata. Emme kuitenkaan tämän työn puitteissa ryhtyneet ratkaisemaan haavoittuvuuksia, sillä palvelin ja järjestelmät ovat vain testikäytössä.

Testien tarkoituksena oli lähinnä vain kokeilla minkälaisia tuloksia molemmat järjestelmät antavat ja saada hiukan perspektiiviä siitä, että kuinka turvalliseksi nämä järjestelmät voidaan yleisesti ottaen kuvailla. Mielestämme järjestelmät ovat kohtalaisen turvallisia, mikäli korkeanluokan riskejä ei ole ja keskiluokan riskejä on vain muutamia. Esimerkiksi samankaltaisia tuloksia tuli aiemmin kotikoneesta, jossa oli käyttöjärjestelmänä Windows 7 uusimmilla päivityksillä, palomuri ja ajan tasalla oleva virustorjuntaohjelmisto.

9 KÄYTTÖKOKEMUKSET JÄRJESTELMISTÄ

Seuraavat kappaleet perustuvat täysin omiin mielipiteisiin, joita olemme saaneet molemmista järjestelmistä niiden käyttämisen ja testauksen aikana. Kummassakin sekä Windows Home Serverissä että Amahi Home Serverissä on omat haittansa ja etunsa. Esittelemme niitä tässä kappaleessa puolueettomasti mutta nojaten kuitenkin omiin käyttökokemuksiin. Nämä voivat olla tietysti erilaisia riippuen käyttäjästä, kokemuksesta ja laitteistosta.

9.1 Haitat

Ensimmäiseksi mainitsemme molempien järjestelmien huonot puolet. Windows Home Server on maksullinen. Tämä on siksi huono puoli, koska Amahi Home Server on ilmainen.

WHS:ssä on toisinaan kummallisia ongelmia jakokansioiden oikeuksissa. Käyttäjä ei päässyt välillä esimerkiksi Pictures-kansioon hallintakonsolin kautta eikä myöskään suoraan Windowsin lähiverkon kautta, vaikka sinne oli asetettu täydet oikeudet. Ongelmista päästiin kuitenkin eroon, kun asetettiin samat käyttäjätunnukset ja salasanat sekä palvelimen että asiakaskoneen tunnuksiin. Mielestämme tämä oli rasittava ongelma, sillä kun käyttäjälle asetetaan oikeudet jakokansioihin palvelimelta, pitäisi niiden toimia aivan normaalisti.

Varmuuskopiointien määrityksessä voi valita pelkästään erikseen ja yksitellen kansiot, jotka halutaan jättää pois varmuuskopioinnista. Tämä on todella huonoa käytettävyyttä, sillä jos kansioita on paljon ja kaikkia ei haluta varmuuskopioida, on tämänkaltainen tapa erittäin aikaa vievää. Olisi paljon kätevämpää ja helpompaa jos kansiot voitaisiin valita samalla kertaa.

Windows-käyttöjärjestelmiä ovat iät ja ajat vaivanneet virukset. Windows Home Server ei ole sen erikoisempi tapaus. Siihenkin löytyy viruksia ja tällöin se olisi hyvä pystyä suojaamaan. WHS:n virustorjuntaohjelmistojen määrä on vielä aika suppea mutta vaihtoehtoja löytyy kuitenkin jonkin verran. Ilmaiset

virustorjuntaohjelmistot eivät ole kovin kummoisia, joten jos haluaa panostaa varmempaan tietoturvallisuuteen, on syytä hankkia maksullinen virustorjuntaohjelmisto.

Windows Home Serverissä median streamaus toimi meidän laitteilla langattoman yhteyden kautta huonosti. Elokuvat eivät pyörineet juuri lainkaan Windows Media Centerissä ja kuva- sekä musiikkitiedostojen selailu ja toisto eivät toimineet kovin sulavasti.

Amahi Home Serverin asentaminen ei ole niin helppoa kuin Windows Home Serverin asentaminen. Voisimme sanoa, että Amahin asentamiseen tarvitsee jonkin verran kokemusta ja tietoa tietokoneista sekä Linux-pohjaisista käyttöjärjestelmistä. Ensinnäkin asentamiseen tarvitaan erilliset ohjeet, jotka löytyvät Amahin sivuilta. Lisäksi asentamista varten täytyy ladata Fedoran DVD-levykuva ja polttaa se DVD:lle. Asennusvaiheessa joudutaan määrittämään tietynlaisia asetuksia, kuten esimerkiksi osoitepolku ohjelmistopaketeille Amahia varten, jotta asennusprosessi onnistuu. Peruskäyttäjän näkökulmasta katsottuna tämä ei ole välttämättä kovin helppoa ja selkeää.

AHS:ssä on sisäänrakennettu hakutoiminto, jolla pystyy hakemaan palvelimella sijaitsevia tiedostoja. Hakutoiminto on keskeneräisen oloinen, sillä päästäksesi esimerkiksi tiettyyn kansioon, tulee tietää kansion nimi, koska niin sanotut valmiit hakulinkit (images, audio, video, files) eivät toimi. Lisättäessä tiedostoja palvelimelle, tulee palvelimella tehdä tietokantapäivitys erikseen ajamalla komentokehoteessa updatedb-komennon, koska muuten AHS:ssä ei näy lisätyt tiedostot. Lisäksi tiedostot eivät aukea hakutulosten kautta Firefoxissa, vaan pelkästään Internet Explorer –selaimessa. Jakokansioiden selaaminen on siis järkevintä tehdä suoraan esimerkiksi Windowsin resurssienhallinnan kautta.

Varmuuskopiointien tekeminen on toteutettu mielestämme huonosti AHS:ssä. Varmuuskopiot piti määrittää asiakaskoneen päästä palvelimeen esimerkiksi käyttäjäkansioon. Tämä on kömpelö tapa, mikäli asiakaskoneita on kotiverkossa monin kappalein. Varmuuskopiointeja varten on olemassa kolmannen osapuolen ohjelmia, joita oli monia vaihtoehtoja. Ne tuntuivat kuvauksien ja kuvakaappausten perusteella kuitenkin vaikeakäyttöisiltä.

Kotisivujen ja etähallinnan käyttöönottoaminen on monimutkaista ja työlästä AHS:ssä. Kotisivuja varten täytyy esimerkiksi muokata muutamia rivejä HTTP-palvelun tiedostoihin. Etähallintaa varten täytyy asiakaskoneeseen asentaa VPN-ohjelmisto, jolla päästään käsiksi palvelimeen kotiverkon ulkopuolelta.

Amahi Dashboardin eli hallintapaneelin käyttöliittymä on mielestämme suppea. Ominaisuuksia ei löydy niin paljoa kuin Windows Home Serveristä eikä hallintapaneeli ole yhtä selkeä ja mukavakäyttöinen. Amahi Home Server kaipaa vielä reippaasti lisää kehitystyötä. Siihen voitaisiin esimerkiksi kehittää samankaltainen ohjelmisto kuin Windows Home Serverissä, joka valvoo muun muassa asiakaskoneiden tiloja.

9.2 Edut

Windows Home Server Console eli hallintapaneeli on miellyttävä, käyttäjäystävällinen ja selkeä. Se on myös näppärästi yhdistetty asiakaskoneisiin, joka tarkoittaa sitä, että Windows-käyttöjärjestelmien tehtäväpalkissa näkyy aina kuvake, joka ilmoittaa sekä palvelimen että palvelimeen yhdistettyjen asiakaskoneiden tilan ja siitä pääsee myös kätevästi palvelimeen käsiksi.

Streamauksessa Windows Media Center –ohjelmisto sulautuu kätevästi palvelimen jakokansioiden kanssa. WHS:ssä on valmiita jakokansioita, kuten esimerkiksi Movies, Music ja Pictures, jotka integroituvat suoraan Windows Media Centeriin. Käyttäjän ei tarvitse huolehtia muusta kuin siirtää vain esimerkiksi videotiedostot Movies-kansioon.

Etähallinta sekä kotisivujen ja domainin luominen on toteutettu hyvin ja yksinkertaisesti. Käyttäjän ei tarvitse periaatteessa kuin asettaa muutamat porttiohjaukset reitittimeen (myös Amahissa) ja määrittää kotisivuosoite WHS:n asetuksista. Näin mahdollistuu myös etähallinta, koska se toimii kotisivujen kautta, josta pääsee sisään kirjautumalla konsoliin.

Aikaisemmin mainittiin jo, että Amahi Home Server on ilmainen. Tämä on tietysti aina hyvä puoli.

AHS pohjautuu Linuxiin eli tarkemmin sanottuna Fedora-distributioon. Se takaa turvallisemman ympäristön, koska esimerkiksi suurin osa tehdyistä viruksista on Windows-käyttöjärjestelmiin. Linux-pohjaiset käyttöjärjestelmät ovat usein myös kevyitä, eivätkä vaadi koneelta tehoja kovin paljoa toimiakseen sulavasti.

Appsien eli lisäominaisuuksien asentaminen on toteutettu hyvin. Se on todella helppoa ja nopeaa, koska se onnistuu suoraan Dashboardin Apps-osiosta löytyvän ohjelmistolistan kautta.

Amahissa streamaus ja sen käyttöönotto oli helppoa ja hyvin toimiva. Täytyi vain asentaa Apps-osiosta muutama ohjelmapaketti, jonka jälkeen streamauspalvelu oli käytettävissä. Windows Media Center toisti langattomalla yhteydellä elokuvat, musiikit ja kuvat todella sulavasti, toisin kuin Windows Home Serverissä.

Apua ongelmiin löytyy esimerkiksi Amahin keskustelupalstoilta. Linux-maailmassa saa yleensä aina asiallisia ja asiantuntevia vastauksia sekä neuvoja monenlaisiin ongelmiin.

9.3 Yhteenveto

Niin kuin aikaisemmin mainitsimme, kummassakin sekä Windows Home Serverissä että Amahi Home Serverissä on omat hyvät ja huonot puolensa. Käyttökokemusten ja testien perusteella kallistumme itse enemmän Windows Home Serverin puoleen, koska siinä on mielestämme kiistatta enemmän hyviä puolia kuin Amahi Home Serverissä.

WHS on paljon viimeistellympi tuote ja huomattavasti mukavampi sekä yksinkertaisempi käyttää. Tämä on ymmärrettävää, koska WHS on kuitenkin kaupallinen tuote. Odotamme silti AHS:ltä tulevaisuudessa paljon, mikäli sitä saadaan kehitettyä. Ilmaiseksi tuotteeksi se on kuitenkin hyvä, ja mikäli jaksaa tarpeeksi säätää siitä saa varmasti hyvän järjestelmän.

10 POHDINTA

Työhön olisi mielestämme saanut varsinaisen tutkimusongelman, mikäli siihen olisi ollut toimeksiantaja, kuten esimerkiksi jonkin pienyritys tai joku muu yksityinen henkilö, jossa olisi ollut maksimissaan kymmenen asiakaskoneen lähiverkko. Tällainen olisi ollut ideaali testausympäristö tämänkaltaisille järjestelmille. Kysymyksessä on lähinnä vain tutustuminen kotipalvelinkäyttöjärjestelmiin sekä näiden testausta ja vertailua, joiden perusteella saimme mielikuvan, että kumpi näistä olisi parempi meidän mielestä kotikäyttöön.

Opinnäytetyön aloittaminen tuntui melko vaikealta, koska emme ensinnäkään oikein tiedeet missä työstäisimme opinnäytetyötä ja mistä saisimme tarvittavat materiaalit, kuten esimerkiksi laitteet ja ohjelmistot. Aihe oli todella hankala ja aluksi se koskikin ainoastaan Windows Home Serveriä. Myöhemmin saimme aiheeseen lisää syvyyttä ja selkeyttä lisäämällä aiheeseen toinen samantyyppinen järjestelmä. Näin saimme selkeämmän kuvan siitä miten ryhdymme työstämään aiheitamme.

Törmäsimme matkalla myös muunlaisiin ongelmiin sen jälkeen kun saimme laitteistot ja työtilat koulun laboratorion. Siellä ei ollut esimerkiksi mahdollista suorittaa tarvittavia testejä järjestelmille, joten se oli yksi syy siihen, että päätimme ruveta työstämään opinnäytetyötä kotitiloissa omilla laitteilla. Talvi ja kevät olivat kiireistä aikaa, joten tekeminen jäi todella vähille, jolloin alun perin suunniteltu aikataulu ei pitänyt ollenkaan paikkaansa. Tämä oli toinen syy miksi emme voineet enää tehdä opinnäytetyötä koulun laboratoriossa.

Kesällä tilanne muuttui. Saimme asennettua tarvittavat laitteet ja ohjelmistot kotiin, jolloin vaadittava testausympäristö oli valmis. Siitä eteenpäin opinnäytetyön tekeminen on sujunut sulavasti ja nopeasti.

Työssämme käytettiin tietoturvallisuuden testaamiseen Nessus-testaustyökalua. Perustelut tälle löytyy muun muassa siitä, että työkalusta oli aikaisempaa kokemusta harjoitustyön muodossa, joten se oli jo ennestään tuttu.

Lisäksi Nessus on rankattu esimerkiksi sectools.org –sivuston mukaan parhaimmaksi tietoturvatyökaluksi. (Top 100 Network Security Tools, hakupäivä 30.8.2010.) Myös monella muulla Internet-sivulla Nessusta on keuhuttu parhaaksi työkaluksi tietoturvan testaamiseen.

Opinnäytetyön tekeminen kokonaisuudessaan oli kuitenkin ihan mielenkiintoista ja mukavaa, koska siinä sai uutta kokemusta ja tietoa meille uusista järjestelmistä. Saimme työstämisen aikana myös ajatuksen valjastaa kotipalvelinjärjestelmän mahdollisesti omaan käyttöön tulevaisuudessa. Jäämme innolla odottelemaan, miten kotipalvelinkäyttöjärjestelmät kehittyvät vielä ja rupeavatko ne yleistymään kotikäytössä.

LÄHTEET

Anderson, H. Introduction to Nessus. Hakupäivä 2.4.2010,
<http://www.symantec.com/connect/articles/introduction-nessus>

Edney, A. 2007. Windows Home Server User's Guide. Berkeley: Apress.

Feature Gallery for the Amahi Home Server. Hakupäivä 14.2.2010,
<http://www.amahi.org/features/gallery>

Features of The Amahi Home Server. Hakupäivä 8.2.2010,
<http://www.amahi.org/features>

Hallihan, R. 2008. Windows Home Server: Protect And Simplify Your Digital Life. Indianapolis: Wiley Publishing Inc.

Hartikainen, J. Nessus Tietoturvan tarkastamisohjelma. Hakupäivä 24.3.2010,
<https://jyx.jyu.fi/dspace/handle/123456789/19986>

Kettel, G & J. 2008. Windows Home Server Bible. Indianapolis: Wiley Publishing Inc.

McFedries, P. 2009. Microsoft Windows Home Server Unleashed. Indianapolis: Sams Publishing.

Most Popular Windows Home Server Add-ins. Hakupäivä 18.6.2010,
<http://www.microsoft.com/windows/products/winfamily/windowshomeserver/add-ins.aspx>

Top 100 Security Tools. Hakupäivä 30.8.2010,
<http://sectools.org/>