24.2.2007

LAPPEENRANNAN
TEKNILLINEN YLIOPISTO

Teknistaloudellinen tiedekunta
Tietotekniikan osasto
Tietotekniikan laitos
Ti5316800 - Lähiverkot - erikoistyökurssi

Linux-työ:
Backup - Varmuuskopiointi

0237513

Kemppainen Ossi

Tietotekniikka 4

SISÄLLYSLUETTELO

LYHENNELUETTELO

AES	Advanced Encryption Standard
AMANDA	Advanced Maryland Automatic Network Disk Archiver
AWK	Aho, Weinberger, and Kernighan
RAID	Redundant Array of Inexpensive Disks
RSH	Remote Shell
SSH	Secure Shell
TAR	Tape Archive

1 JOHDANTO

Tämä harjoitustyö on tehty Lappeenrannan teknillisin yliopiston tietotekniikan laitoksen Lähiverkot erikoistyökurssin Linux-harjoitustyönä. Aiheena työssä on Varmuuskopiointi. Työssä käsitellään ensin varmuuskopiointia yleisesti; esitellään varmuuskopiointityyppejä ja varmistustrategioita. Tämän jälkeen käsitellään varmuuskopioinnin perusteita, jossa käydään läpi lyhyesti varmuuskopioinnin tärkeyttä ja minkälaisia tiedostoja kannattaa yleisesti varmistaa. Lisäksi samassa yhteydessä käydään läpi varmuuskopioiden säilyttäminen, palauttaminen ja varmuuskopiointiprosessi, sekä esitellään hyvän varmuuskopiointiohjelman ominaisuuksia.

Työn käytännön osuudessa esitellään lyhyesti kolme varmuuskopiointiohjelmaa, joista valitaan yksi kurssilla toteutettavaan yritysverkkokokoonpanoon. Toteutettavassa osuudessa käydään läpi itse ohjelmien asentaminen, konfigurointi ja käyttäminen. Lisäksi työn lopussa esitellään, kuinka toteuttaa oma skripti-pohjainen varmuuskopiointiratkaisu.

2 YLEISTÄ VARMUUSKOPIOINNISTA

Varmuuskopioinnilla tarkoitetaan tiedostojen ja hakemistojen kopioimista tai kahdentamista alkuperäisestä lähteestä toiseen paikkaan niin, että kopioidut tallenteet ovat palautettavissa tai saatavissa takaisin alkuperäiseen paikkaan tai jopa muuallekin. Varmuuskopiointia käytetään tyypillisesti erilaisten ongelmien varalle, kuten esimerkiksi laiterikkojen, erilaisten virhetilanteiden (ohjelmien tai käyttäjän virheet) sekä katastrofien varalle. Varmuuskopioinnin avulla voidaan taata tietty turvallisuustaso, sillä varmuuskopioista tieto on edelleen saatavissa, vaikka alkuperäinen tieto tuhoutuisikin. Varmuuskopioiden ottaminen alkuperäisistä tiedostoista ja hakemistoista on tapahduttava riittävän usein, eli tyypillisesti aina kun tietoa muutetaan, jotta varmuuskopiointi olisi mahdollisimman hyödyllistä. Kuitenkaan tämä ei ole käytännössä aina mahdollista, jonka vuoksi onkin hyvä suunnitella oma varmuuskopiointistrategia kuhunkin tilanteeseen ja tarpeeseen.

2.1 Varmuuskopiointityypit

Varmistusstrategiat perustuvat tyypillisesti lähes aina kolmeen varmuuskopiointitapaan. Tavat voidaan luokitella seuraavasti; täysi varmistus, inkrementaalinen varmistus sekä differentiaalinen varmistus. Niiden pääasiallinen ero toisiinsa on niiden varmistustavassa eli mitä milloinkin varmistetaan.

Täydessä varmistuksessa varmistetaan koko tiedostojärjestelmä tai jokin tietty kokonainen osio järjestelmästä. Täysi varmistus on tyypillisesti järjestelmän ylläpidon perustoimi. Hyvänä puolena täydessä varmistuksessa on se, että kaikki tiedostot ja kansiot varmistuvat kerralla. Kuitenkin huonona puolena voidaan pitää sitä, että se vie paljon tallennusresursseja ja aikaa. Tämän vuoksi täysi tallennus suoritetaankin silloin, kun järjestelmän kuormitus on minimissään eli tyypillisesti yöaikaan. Lisäksi yöaikaan järjestelmien käyttö ja tiedostojen muuttuminen on tyypillisesti varsinkin yrityskäytössä melko vähäistä. (Durham 2002, s.332)

Inkrementaalinen varmistus tarkoittaa varmistusmenetelmää, jossa kopioidaan ainoastaan ne tiedostot ja kansiot, jotka ovat muuttuneet tai jotka on luotu edellisen täyden, differentiaalisen tai inkrementaalisen varmuuskopioinnin jälkeen. (Durham 2002, s.332). Käytettäessä täyttä ja

inkrementaalista varmistusta rinnakkain, etuna on se, että itse varmistusprosessi vie vähän aikaa, sillä muuttuneet tiedostot saadaan kopioitua nopeasti talteen. Huonona puolena voidaan pitää sitä, että varmuuskopioiden palauttaminen voi olla suuritöinen urakka. Palauttamisessa nimittäin joudutaan palauttamaan sekä edellinen täysi varmistus, että kaikki sen jälkeen suoritetut inkrementaaliset varmistukset. (Durham 2002, s.332)

Differentiaalisessa varmistuksessa varmuuskopioidaan kaikki täyden varmistuksen jälkeen muutetut tai luodut tiedostot ja kansiot. Varmistusprosessi vaatii enemmän tallennusresursseja kuin inkrementaalinen varmistus, mutta kuitenkin vähemmän kuin täysi varmistus. Käytettäessä täyttä ja differentiaalista varmistusta rinnakkain, etuna on se, että varmuuskopioiden palautusprosessi on nopeampi (verrattuna pelkkään täyteen varmuuskopiointiin) ja palautuskertoja on vähemmän (verrattuna inkrementaaliseen varmuuskopiointiin). (Durham 2002, s.332)

Näiden varmuuskopiointityyppien lisäksi on vielä peilaus-varmuuskopiointi (mirror backup). Se on identtinen täyden varmuuskopioinnin kanssa, mutta peilaus-varmuuskopiointia ei pakata millään tavalla. Toisin sanoen peilaaminen tekee identtiset kopiot alkuperäisistä tiedostoista ja kansioista ilman mitään pakkauskompressointia.

2.2 Varmistusstrategiat

Varmistusstrategioilla tarkoitetaan yksinkertaisesti varmistusohjelman, -tyypin sekä -ajankohdan valintaa varmistusjärjestelmälle. Varmistusstrategia kannattaa aina luoda omia tarpeita ja resursseja vastaavaksi kokonaisuudeksi. Varmistusohjelman valintaan pitää kiinnittää aina riittävästi huomiota, sillä huonosti valittu ohjelma ei palvele sen käyttäjiä eikä myöskään sen ylläpitäjiä. (Durham 2002, s.333) Varmistusstrategioiden suunnitteluun kuuluu lisäksi itse varmuuskopioiminen, kopioiden säilyttäminen ja palauttaminen, joista lisää kappaleessa kolme, Varmuuskopioinnin perusteet.

Varmistusstrategiaan tärkeänä osana kuuluu varmistustyypin valinta ja sen oikea ajoittaminen. Tyypillisesti täyden varmistuksen tueksi valitaan joko inkrementaalinen tai differentiaalinen varmistus. Näin voidaan helpottaa itse varmuuskopioiden palautusprosessia sekä varmuuskopiointiresursseja. Esimerkiksi jos valitaan harvoin tapahtuvat täydet varmistukset ja

usein tapahtuvat differentiaaliset varmistukset, tarvitsee vain palauttaa viimeisin differentiaalinen varmistus täyden varmistuksen lisäksi. Kuitenkin tämä differentiaalinen varmistus voi vaatia paljon varmistusresursseja järjestelmältä. Jos puolestaan valitaan harvoin tapahtuvat täydet varmistukset ja usein tapahtuvat inkrementaaliset varmistukset, tällöin on palautettava kaikki inkrementaaliset varmistukset täyden varmistuksen lisäksi. Inkrementaalinen varmistus ei vie paljoa varmistusresursseja järjestelmältä. Jeff Durman ehdottaakin kirjassaan, että yleisesti suositeltavaa on suorittaa täysi varmistus kerran viikossa ja inkrementaalinen varmistus päivittäin. Tällainen varmistusratkaisu sopisi esimerkiksi yrityksen toimistotietokoneiden varmistukseen. Täysi varmistus kannattaa suorittaa tyypillisesti sellaisena viikonpäivänä, jolloin järjestelmän käyttö on vähäistä eli esimerkiksi viikonloppuisin, riippuen tietenkin kyseessä olevasta järjestelmästä ja toimintaympäristöstä. (Durham 2002, s.333) Esimerkiksi vedonlyöntipörssin ja toimistoympäristön varmuuskopiointijärjestelmät ja niiden ajoitukset ovat hyvinkin erilaisia.

Kaikkien varmistusstrategioiden toteuttaminen on usein aikaa, vaivaa ja rahaa vievä prosessi. Yksi tehokkaimmista varmistusstrategioista on varmistaa tiedot heti, kun ne ovat luotuna. Tällaisen varmistuksen tekee tietojen peilaus, joka tallentaa tiedot reaaliaikaisesti kahteen paikkaan yhden sijaan. Toinen paikka on yleensä tietokoneen toinen kiintolevy. Tätä voidaan kutsua vikasietoiseksi ratkaisuksi, sillä jos toinen kiintolevy vioittuu, toinen astuu käyttöön, kunnes viallinen kiintolevy on vaihdettu ehjäksi. (Durham 2002, s.333)

Kiintolevyn peilaaminen on eräs Redundant Array of Inexpensive Disks -menetelmistä. Se ei ole kuitenkaan varsinaisesti varmuuskopiointimenetelmä vaan tietokoneiden vikasietoisuutta kasvattava metodi. Levyn peilaus on edustaa tyypiltään RAID 1 -järjestelmää, jossa on useita kiintolevyjä. Siinä sama tieto tallennetaan useisiin kiintolevyihin, jotta saataisiin aikaiseksi mahdollisimman vikasietoinen järjestelmä, ja nopeat levyn tallennus- ja lukuoperaatiot. Toinen järjestelmä on puolestaan RAID 5, jossa käytetään myös useita kiintolevyjä, mutta yhtä niistä käytetään pariteettitarkistukseen. (Durham 2002, s.334) Pariteettitarkistus on menetelmä, jossa lisätään siirrettävään bittijonoon yksi ylimääräinen bitti eli tarkistussumma, jonka avulla voidaan havaita tapahtuneita virheitä. (Laitinen 2004, s. 75) Esimerkiksi RAID 5 -järjestelmässä kiintolevyn vioittuessa, tiedot ovat edelleen saatavissa ja vioittunut levy voidaan korvata uudella levyllä. Kuitenkin jos järjestelmässä kaksi tai useampaa levyä vioittuu, voidaan näin kaikki tiedot menettää. (Durham 2002, s.334)

3 VARMUUSKOPIOINNIN PERUSTEET

Varmuuskopioinnin perusteisiin kuuluvat varmuuskopioinnin merkityksen käsittäminen ja siihen liittyvien alakäsitteiden ymmärtäminen. Alakäsitteet, kuten varmuuskopioiden säilyttäminen ja niiden palauttaminen ovat tärkeä osa koko varmuuskopiointiprosessia. Varmuuskopiointiprosessi on jo itsessään niin keskeinen kokonaisuus, joka on myös hyvä ymmärtää tarkoin. Lisäksi on hyvä tietää nykyaikaisten ja hyvien varmuuskopiointiohjelmien perusominaisuuksia.

3.1 Varmuuskopiointi

Miksi varmuuskopioida?

Varmuuskopioinnille on monia eri syitä ja tekijöitä, joiden vuoksi varmuuskopiointia kannattaa suorittaa. Pääsyynä voidaan pitää sitä, että tietoja ei haluta menettää. Tietojen menettämiseen on neljä perussyytä, joiden vuoksi pitää varmuuskopioida: laiteviat, ohjelmavirheet, ihmisen oma toiminta tai luonnon onnettomuudet. (Durham 2002, s.334) Laiteviat ovat tyypillisin käyttäjiä koskettava ongelma, sillä tietokonelaitteet ovat herkkiä rikkoutumaan. Varsinkin tietokoneen kiintolevyt, jossa itse tietoa säilytetään, voivat rikkoutua jopa itsestään tai vanhuuttaan. Myöskään kaikki tietokoneohjelmat eivät ole luotettavia, sillä ne voivat huonosti toimiessaan hävittää käyttäjän omia tietoja ja dataa. Tiedoilla tarkoitetaan tässä yhteydessä käyttäjän henkilökohtaisia salasanoja sekä käyttäjätunnuksia. Datalla tarkoitetaan puolestaan käyttäjän henkilökohtaisia tiedostoja, kuten esimerkiksi sähköposteja ja dokumentteja. Lisäksi on olemassa viruksia ja muita haittaohjelmia, jotka voivat aiheuttaa tiedostojen tuhoutumisia. Tämän vuoksi ihmisen oma toiminta on kriittisessä asemassa, sillä ihmiset voivat joko vahingossa, tietämättään tai tarkoituksella hävittää tärkeitä tietoja tietokoneiltaan. Lisäksi on olemassa luonnon onnettomuuksia, kuten maanjäristykset, tulvat ja tulipalot sekä monet muut katastrofit, jotka voivat aiheuttaa tietojen menettämisiä. Näiden syiden vuoksi, onkin tärkeää harjoittaa säännöllisin väliajoin varmuuskopiointia.

Mitä varmuuskopioida?

Yleensä kaikkia mahdollisia tiedostoja ei kannata varmuuskopioida, se yksinkertaisesti vie liikaa tallennusresursseja, rahaa ja aikaa. Tämän vuoksi kannattaakin valita juuri itsellensä, yritykselle tai järjestelmälle tärkeimmät tiedostot ja kansiot varmennettavaksi. Pääperiaatteena voidaan pitää

sitä, että tärkeimpiä tiedostoja ovat ne, joita ei voida korvata tai ei pystytä uudelleen tekemään helposti. Niinpä ennen varmuuskopiointia onkin hyvä tehdä luettelo varmuuskopioitavista tiedostoista. Seuraavassa on esimerkkilista tiedostoista, jota yksityiskäyttäjän olisi syytä harkita varmuuskopioitavaksi. Kuitenkaan kaikkia näitä ei välttämättä voida varmuuskopioida käyttöjärjestelmästä erillään.

- Pankkitositteet ja muut tilitiedot
- Digitaaliset valokuvat
- Internetistä ostetut ja ladatut ohjelmistot sekä musiikit
- Työ projekteihin liittyvät tiedostot
- Koulunkäyntiin liittyvät tiedostot
- Sähköpostit ja sähköpostin osoitekirjat
- Selaimen kirjainmerkit
- Muut omat tärkeät kansiot

3.2 Varmuuskopioiden säilytys

Varmuuskopiot kannattaa aina sijoittaa erilleen itse kopioitavista tiedoista. Näin saadaan aikaan mahdollisimman vikasietoinen ratkaisu, joka palvelee niin varmuusjärjestelmän käyttäjiä kuin ylläpitäjiäkin. Varmuuskopioiden säilyttämiseen on valittavana useita eri tallennusvaihtoehtoja. Tyypillisimmät näistä ovat kiintolevy, nauha ja CD/DVD-levyt. Hieman uudempia vaihtoehtoja ovat ulkoiset USB-kiintolevyt sekä verkossa olevat tallennuspalvelut. Kiintolevyt ja nauhat ovat varsin edullisia, melko luotettavia ja nopeita tallennusvaihtoehtoja (Koski. 2000, s.108). Tämän vuoksi niitä käytetään varsinkin yrityskäytössä paljon. CD/DVD-levyt puolestaan soveltuvat hyvin yleis- ja yksityiskäyttöön, sillä ne ovat helppokäyttöisiä ja melko nopeita. USB-kiintolevyt ovat myös saavuttaneet yksityiskäytön varmuuskopioinnissa, sillä ne ovat usein todella helppokäyttöisiä ja niissä on paljon tallennuskapasiteettia. (Microsoft 2004) Uutena vaihtoehtona varmuuskopioiden säilyttämiseen ovat verkossa olevat tallennuspalvelut ja tietovarastot. Niitä hyödyntämällä sinne voidaan varmuuskopioida suuriakin määriä tietoja, mutta samalla kustannukset nousevat myös suuriksi. (Microsoft 2004) Tällaisia tietovarastoja hyödynnettäessä on otettava huomioon tietoturvalliset seikat sekä tietojen säilyvyyden luotettavuus.

Tallennusvaihtoehdon valinta on yksi tärkeimmistä päätöksistä liittyen varmuuskopiointiin. Valinnassa on otettava huomioon niin kustannukset, luotettavuus, nopeus, saatavuus kuin käytettävyyskin (Koski. 2000, s.108). Jokainen ominaisuus on punnittava tarkkaan, sillä on tiedettävä tarkalleen, mitä varmuuskopiointijärjestelmä halutaan. Esimerkiksi varmuuskopioiden säilyttämisen ja varmistuksen kustannukset eivät saa nousta suuremmaksi kuin itse varmuuskopioitavan tiedon arvo on. Luotettavuus on myös yksi tärkeimmistä varmuuskopiointijärjestelmän perusominaisuuksista, josta ei kannata tinkiä. Luotettavuudella tarkoitetaan tässä yhteydessä järjestelmän vakaata toimivuutta kaikissa tilanteissa. Järjestelmän nopeus puolestaan ei ole niin tärkeä ominaisuus, sillä tyypillisesti varmuuskopiot kyllä ehditään ottamaan ajoissa. Henkilökohtaisessa varmistuksessa kuitenkin varmuuskopiointinopeus voi olla hyvinkin kriittinen tekijä. Varmuuskopioiden helppo saatavuus ja järjestelmän hyvä käytettävyys ovat perusominaisuuksia, joista ei myöskään kannata tinkiä. (Koski. 2000, s.108)

Varmuuskopioiden säilyttämiseen liittyy myös kopioiden versionhallinta ja niiden tietty säilyttämisaika. Tyypillisesti varmuuskopioista kannattaa säilyttää vähintäänkin noin 4-5 eri versiota, joita uusitaan aina uuden varmuuskopiointikerran yhteydessä.

3.3 Varmuuskopioiden palauttaminen

Varmuuskopioiden palauttamisella tarkoitetaan otettujen kopioiden kopioimista eli palauttamista takaisin alkuperäiseen paikkaan tai johonkin muualle haluttuun paikkaan. Palautusprosessi voidaan yleensä suorittaa joko varmuuskopiointiohjelmalla tai manuaalisesti käsin.

Monissa kehittyneissä varmuuskopiointiohjelmissa on ominaisuus, jonka avulla varmuuskopiot voidaan palauttaa haluttuun paikkaan nopeasti ja helposti. Tämä tapahtuu tyypillisesti jollakin tietyllä komennolla tai pikakuvakkeella. Käyttämällä ohjelman omaa palautusoperaatio-ohjelmaa, käyttäjän ei tarvitse miettiä esimerkiksi tar tai zip tiedostojen purkukäskyjä. Varmuuskopiointiohjelmien palautusoperaatiolla säästetään aikaa ja vältetään mahdollisia virheellisiä palautuksia.

Manuaalisesti tapahtuva palauttaminen tarkoittaa varmuuskopioiden kopioimista käsin, tietyllä komennolla (esimerkiksi cp = copy) tai purkukäskyllä (esimerkiksi tar xzvf …) haluttuun

paikkaan. Käytettäessä manuaalista palautusoperaatiota, on käyttäjän oltava tarkkana, ettei vahingossa pura varmuuskopiota väärään paikkaan tai muuten vahingoita varmuuskopioita.

3.4 Varmuuskopiointiprosessi

Varmuuskopiointiprosessilla tarkoitetaan kokonaisuutta, jossa käydään kaikki varmuuskopioinnin perusvaiheet lävitse. Ensimmäinen vaihe prosessissa alkaa, kun käyttäjä miettii, mitä, miten ja milloin varmuuskopioidaan, sekä mihin varmuuskopiot tallennetaan. Tämän jälkeen on itse varmuuskopioiden ottaminen, jonka jälkeen varmuuskopioiden säilyttäminen ja niiden mahdollinen palauttaminen. Ennen varmuuskopiointiprosessin alkua käyttäjä on valinnut ja asentanut itselleen sopivan varmuuskopiointiohjelman.

Esimerkkinä varmuuskopiointiprosessista voidaan esitellä yksityiskäyttäjälle soveltuva tapaus. Tässä tapauksessa yksityiskäyttäjä haluaa ottaa tietokoneeltaan kaikista valokuvistaan sekä dokumenteistaan varmuuskopiot. Kopiot otetaan Windows käyttöjärjestelmälle soveltuvalla varmuuskopiointiohjelmalla, nimeltään Backup4all. Varmuuskopiot halutaan tallennettavaksi käyttäjän omalle USB-kovalevylle. Käyttäjä haluaa myös, että varmuuskopiointi tapahtuisi säännöllisesti aina joka maanantaiaamu kello kahdeksan.

Varmuuskopiointiohjelmalla voidaan määritellä tarkasti, mitä kopioidaan ja minkä tyyppisiä varmuuskopioita käytetään. Tässä tapauksessa voidaan määritellä, että varmuuskopiointiohjelma kopioi ja pakkaa suosituimmat kuvaformaatit (jpg, jpeg, png, gif, ja bmp) ja dokumentit (doc, txt, ppt ja xls) talteen. Varmuuskopioiden pakkaamiseen voidaan käyttää esimerkiksi zip-tyyppistä pakkausmetodia. Varmuuskopioiden ottaminen voidaan ajastaa niin, että täysi varmuuskopio otetaan kuvista ja dokumenteista joka kuukauden ensimmäisenä maanantaiaamuna kello kahdeksan. Lisäksi joka viikon maanantaiaamuna otetaan differentiaalinen varmuuskopio muuttuneista kuvista ja dokumenteista. Varmuuskopioita otetaan differentiaalisina, koska käyttäjä haluaa palautusprosessin olevan mahdollisimman nopeaa. Varmuuskopiot tallennetaan aina käyttäjän ulkoiselle USB-kovalevylle, joka vaihdetaan uuteen joka kolmas vuosi, välttäen mahdolliset laitteen vanhuudesta johtuvat laiterikot. Varmuuskopioiden palauttaminen tapahtuu itse varmuuskopiointiohjelmalla, jonka avulla voidaan määrätä tarkasti, mihin varmuuskopiot halutaan palautettavan. Näin varmuuskopiointiprosessi on käyty läpi alusta loppuun.

3.5 Hyvän varmuuskopiointiohjelman ominaisuudet

Varmuuskopiointiohjelman valintaan kannattaa aina kiinnittää paljon huomiota. Ohjelmalla täytyy olla tietyt perusominaisuudet, jotta sitä kannattaa edes harkita käyttöön otettavaksi. Perusominaisuuksina voidaan pitää jo edellä esitetyt toiminnot, kuten luotettava varmuuskopioiminen, helppo palauttaminen sekä tiedon pakkaaminen. Lisäksi monen tallennusmedian valinta kuuluu varmuuskopiointiohjelmien perusominaisuuksiin.

Nykyaikaisilla varmuuskopiointiohjelmilla on perusominaisuuksien lisäksi monia lisäominaisuuksia, jotka helpottavat osaltaan varmuuskopiointia ja tietojen hallintaa sekä säilyttämistä. Seuraavassa on esiteltynä muutamia tärkeimpiä lisäominaisuuksia hyvälle varmuuskopiointiohjelmalle:

Varmuuskopiointityypit (Backup Types)
Ohjelmassa voidaan valita joko täysi, differentiaalinen, inkrementaalinen tai peilaus -tyyppinen varmuuskopiointimenetelmä. Lisäksi varmuuskopiointityyppejä voidaan vaihdella tehtäväkohtaisesti keskenään.

Tiedostofiltterit (File Filters)
Tiedostofiltterit ovat tiedostosuodattimia, joiden avulla voidaan suodattaa tiedostoja esimerkiksi tiedostotyypin, -koon, päivämäärän ja nimen mukaisesti. Suodattimia käytetään esimerkiksi, kun halutaan ottaa varmuuskopio jostakin tietynlaisista tiedostoista.

Sisäänrakennettu aikataulutus (Built-in Scheduler)
Aikataulutuksella voidaan ajastaa varmuuskopiointi tapahtumaan tietyin väliajoin ja tietyin ajanhetkin. Aikataulutuksen avulla käyttäjän ei tarvitse itse huolehtia varmuuskopioinnin käynnistämisestä.

Sähköpostin lähettäminen (Email notifications)
Sähköpostin lähettämisellä tässä yhteydessä tarkoitetaan sitä, että varmuuskopiointiohjelma kykenee lähettämään järjestelmän ylläpitäjälle sähköpostia. Sähköpostia voidaan esimerkiksi lähettää tilanteessa, kun varmuuskopiointiprosessi on joko onnistunut tai epäonnistunut, tai siinä on sattunut virheitä.

Advanced Encryption Standard -salaus (AES encryption)

Monet varmuuskopiointiohjelmat tukevat nykyään kehittyneitä salaus standardeita, kuten 128-, 192- ja 256-bittistä salausmekanismia. Numerot viittaavat salausavaimen kokoon, jolla salataan tietoa. Isompi numero takaa yleisesti paremman salausturvan.

Statistiikat ja lokit (Statistics and logs)

Statistiikat ja lokit antavat tietoa varmuuskopiointiohjelman käyttäjälle ohjelman kopiointi- ja palautusprosesseista. Tiedot koskevat prosessien käynnistämistä, kulkua, onnistumista ja päättymistä. Lokitiedoissa on myös mukana tallennuspaikat, tiedostojen koot, päivämäärät sekä kellonajat.

Salasanaturva (Password Protection)

Salasanaturvan avulla varmuuskopioihin voidaan laittaa salasana, jonka avulla ainoastaan ohjelman käyttäjät ja ylläpitäjät voivat aukaista varmuuskopiot. Salasana voidaan laitettaa tyypillisesti pakattuihin varmuuskopiotiedostoihin.

Varmuuskopioiden jakaminen (Disk Spanning)

Varmuuskopioiden jakamisella tarkoitetaan sitä, että varmuuskopioita voidaan pilkkoa halutun kokoisiksi tiedostoiksi. Tämä on erityisen kätevä toimenpide, kun varmistusmediana on CD:t ja DVD:t. Tällöin voidaan määrätä varmuuskopion maksimikoko, jota ohjelma ei ylitä ja tekee näin määrätyn kokoisia varmuuskopiointitiedostoja. Tiedostot jaetaan usein jollakin pakkausohjelmalla, kuten zip tai tar.

4 VARMUUSKOPIOINTIOHJELMAT

Valitsin työhöni kolme erilaista varmuuskopiointityökalua esiteltäväksi. Ohjelmat edustavat niin suuren, keskisuuren kuin pienenkin tietojärjestelmän varmuuskopiointisysteemiä. Pienemmän luokan työkaluja ovat tar, dump ja cpio, kun puolestaan keskisuuren järjestelmän ohjelmia edustaa Flexbackup. Isojen järjestelmien varmuuskopiointia voidaan hoitaa esimerkiksi Amanda ohjelmalla. Kaikki esittelemäni ohjelmat ovat ilmaisia ja niitä hyödynnetään varsinkin UNIX-pohjaisissa käyttöjärjestelmissä.

4.1 Tar, dump ja cpio

Tar, dump ja cpio kuuluvat Linuxin vakiovarmistustyöluihin. Nämä kolme ohjelmaa ovat eri UNIX-työkaluja, mutta käsittelen ne tässä työssä yhtenä kokonaisuutena, koska ne ovat niin samantyyppisiä ominaisuuksiltaan. tar-apuohjelma suunniteltiin alun perin tiedostojen arkistointiin nauha-asemalle. Nykyisin sitä käytetään Web-arkistotiedostojen luontiin sekä ohjelmien tallennukseen varmuuskopioinnin lisäksi. (Durham 2002, s. 334) tar ja cpio työkalut ovat hyvin samankaltaisia ja yleensä melko samanarvoisia varmistuksen kannalta. Molemmat ohjelmat ovat tarkoitettu tiedostojen arkistointiin, mutta ne toimivat yhtä hyvin myös tiedostojen varmistuksessakin. Molempien perusominaisuuksiin kuuluu tiedostojen tallettaminen nauhalle ja niiden palauttaminen sieltä. Lisäksi molemmat työkalut voivat hyödyntää melkein mitä tahansa tallennusvälineitä, sillä UNIX:n ytimen laiteajurit hoitavat matalan tason laitekäsittelyn. Näin kaikki laitteet yleensä näkyvät samanlaisina käyttäjätason ohjelmille. Kuitenkin komentojen tar ja cpio UNIX-versioilla voi olla joitain ongelmia epätavallisten tiedostojen kanssa. Tällaisia tiedostoja voivat olla esimerkiksi symboliset linkit, laitetiedostot sekä tiedostot, joilla on pitkä polkunimi, mutta R. Kosken mukaan jo vuoden 2000 Linux-versioiden pitäisi käsitellä kaikkia tiedostoja oikein. (Koski 2000, s. 108)

dump-työkalu on hieman erilainen, sillä se lukee tiedostojärjestelmää suoraan eikä vain tiedostojärjestelmän kautta. Lisäksi se on kirjoitettu erityisesti varmistuksia varten. Lukeminen suoraan tiedostojärjestelmästä tuo muutamia etuja. Se sallii tiedostojen varmistamisen ilman aikaleimojen muuttamista. Lisäksi tiedostojärjestelmän suora luku on tehokkaampaa jos tehdään täysi varmistus, sillä se voidaan tehdä vähemmin levyn lukupään liikkein. Kuitenkin dump-työkalun suurin haitta on, että se tekee varmistusohjelman tiedostojärjestelmäkohtaiseksi, sillä

dump-ohjelma ymmärtää vain ext2-tiedostojärjetelmää. Taulukossa 1 on vertailtu näiden kolmen ohjelman eräitä ominaisuuksia. Taulukosta voidaan nähdä, että ohjelmat ovat melko samankaltaisia, mutta eroavaisuuksiakin löytyy.

Taulukko 1. tar, cpio ja dump -ohjelmien vertailua. (Safari Books 2006)

Ominaisuus	tar	cpio	dump
Helppokäyttöisyys	Hyvin yksinkertainen	Yksinkertainen(täytyy määritellä muutamat vaihtoehdot)	Yksinkertainen (täytyy määritellä muutamat vaihtoehdot)
Erikoistiedostojen varmuuskopiointi	Myöhemmissä versioissa	Kyllä	Kyllä
Multivolume varmuuskopiointi	Myöhemmissä versioissa	Kyllä	Kyllä
Varmuuskopiointi verkon yli	Käyttämällä rsh/ssh:ta	Käyttämällä rsh/ssh:ta	Kyllä
Liittää tiedostoja varmuuskopiointiin	Kyllä (tar -r)	Ei	Ei
Tiedostojen listaus varmuuskopioinnin jälkeen	tar cvf 2> logfile	cpio -v 2> logfile	Vain varmuuskopioinnin jälkeen palautuksen yhteydessä
Varmuuskopiointi kriteerin mukaan	Kyllä, GNU tar:ssa	find voi löytää useit kriteereitä	Ei
Tiedostosysteemin tehokkuus	Hyvä	Huonoin	Paras

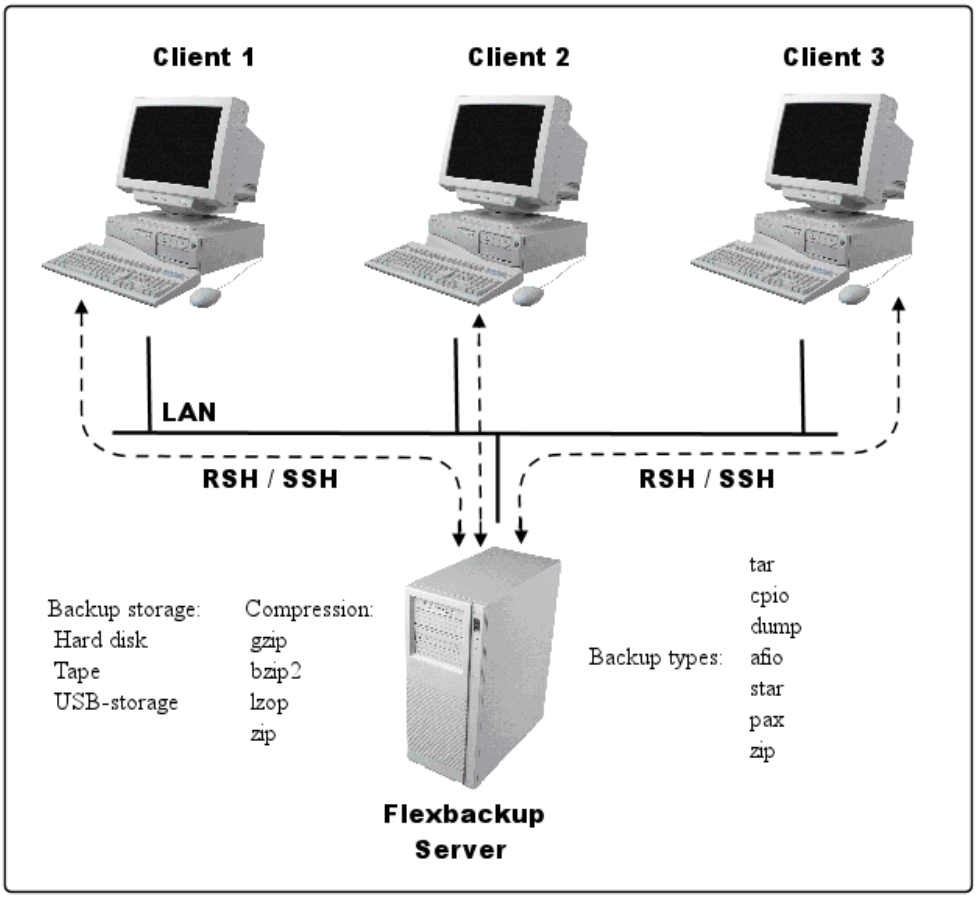
4.2 Flexbackup

“Flexbackup is for you if you have a single or small number of machines, Amanda is "too much", and tarring things up by hand isn't nearly enough...” (Flexbackup 2003)

Flexbackup on ilmainen varmuuskopiointiohjelma. Se on tarkoitettu joko yksittäiselle tietokoneelle tai pienelle määrälle verkossa olevia tietokoneita. Flexbackup on perl-ohjelmointikielellä kirjoitettu ohjelma ja se hyödyntää monia UNIX:ssa olevia valmiita kirjastoja sekä työkaluja. Sen varmuuskopiointi perustuu jo edellä esiteltyihin ohjelmiin, tar, cpio ja dump sekä muihin työkaluihin, kuten afio, star, pax ja zip. (Flexbackup 2003) afio-työkalu on muunnelma cpio-ohjelmasta; afio pakkaa jokaisen tiedoston erikseen (Koski 2000, s. 115). star-työkalu on puolestaan paranneltu ja nopeampi versio tar-ohjelmasta, sen toiminnallisuutta on hieman kehitetty ja se on tarkoitettu pelkästään nauhoille. (Linux About 2007 A) pax on ohjelma, joka lukee ja kirjoittaa tiedostoja ja kansioita sekä kopioi hakemistoja hierarkioineen

paikasta toiseen. (Linux About 2007 B) zip-ohjelma on perinteinen pakkaus- ja purkuohjelma, jota hyödynnetään lähes kaikissa käyttöjärjestelmissä. (Linux About 2007 C) Lisäksi ohjelman itse tiedostojen kompressointi tapahtuu ohjelmilla gzip, bzip2, lzop sekä zip.

Flexbackup-ohjelma toimii yhden serverin periaatteella, jossa ohjelma asennetaan vain yhteen varmuuskopiointiserveriin (backup server), eikä asiakaskoneille (client) tarvitse asentaa mitään. Ohjelma hakee halutut tiedostot ja kansiot RSH tai SSH -työkalujen (Remote Shell ja Secure Shell) avulla ja pakkaa ne jollakin edellä esitellyillä pakkaustyökaluilla. Varmuuskopiot Flexbackup säilöö joko kiintolevylle, nauhalle tai ulkoiseen USB-asemaan. Tämä toimintaperiaate on esiteltynä kuvassa 1.



Kuva 1. Flexbackupin toimintaperitaate.

Flexbackup-ohjelmalla on muitakin tärkeitä ominaisuuksia. Ohjelmalla voidaan tehdä niin täysiä, differentiaalisia kuin inkrementaalisia varmuuskopioitakin. Flexbackup tukee myös puskurointia (buffering), kun tiedostoja kopioidaan verkon yli. Lisäksi ohjelmalla voidaan ajaa haluttuja varmuuskopiointisettejä (backupsets) joko yksittäin tai kaikki setit yhtä aikaa. Kopiot otetaan

aina viimeksi tallennetuista tiedostoista. Varmuuskopiosetit voidaan myös ajastaa cron-ohjelman avulla. Varmuuskopioita voidaan myös vertailla ohjelman compare-toiminnolla. Lisäksi Flexbackup:ssa on itsessään palautusvelho (restore wizard), joka palauttaa varmuuskopiot siihen hakemistoon, missä itse varmuuskopiot sijaitsevat. Ohjelmassa on myös melko hyvät lokitiedostot, joista selviää, milloin ja mihin varmuuskopioita on otettu.

4.3 Amanda

Amanda (Advanced Maryland Automatic Network Disk Archiver) on ilmainen varmuuskopiointiohjelma, joka on kehitetty University of Maryland Computer Centerissä. Se hyödyntää varmuuskopioinnissa muun muassa tar (Tape Archive), dump ja awk -komentoja (Aho, Weinberg ja Kenighan). (Durham 2002, s. 336) (Amanda 2007) awk-komento on hyvin käytännöllinen UNIX-komento, sille se lukee dataa oletuksena rivi kerrallaan, valitsee siitä rivit, jotka täsmäävät annettuun merkkijonomalliin ja suorittaa riveille halutut toimenpiteet. awk:ia voidaan myös käyttää datan prosessointiin ja muiden UNIX-komentosovelluksien automatisointiin. (Linux About 2007 D) Hyödyntämällä UNIX:n komentoja ja ohjelmia Amanda osaa itse automatisoida täydet ja inkrementaaliset varmuuskopiot. (Amanda 2007)

Amanda on kokonaisuudessaan tarkoitettu varmuuskopiointiin ja se on suunniteltu käytettäväksi melko suurissa tietojärjestelmissä. Amandan käyttö perustuu yhteen varmuuskopiointipalvelimeen, jossa on nauhan vaihtajalla varustettu nauha-asema, ja johon asennettu Amandan serveriohjelmisto. Lisäksi järjestelmään kuuluu asiakaskoneet (clients), joihin asennetaan Amanadan asiakasohjelmisto. Ohjelmaa voidaan käyttää kaikkien samassa tietoverkossa olevien käyttäjien varmistusratkaisuna, kunhan se on konfiguroitu haluttuihin tietokoneisiin. Amandan serveri konfiguroidaan UNIX-pohjaiseen tietokoneesen ja asiakaskoneet voivat olla esimerkiksi joko UNIX- tai Windows-pohjaisia tietokoneita. Amandan asennukseen ja konfigurointiin on olemassa kattavat manuaalit sekä ohjeet ohjelmiston kotisivuilla: http://www.amanda.org/ (Amanda 2007)

5 FLEXBACKUP VARMUUSKOPIOINTIOHJELMAN ASENNUS, KONFIGUROINTI JA KÄYTTÄMINEN

Valitsin Flexbackup-ohjelman asennettavaksi lähiverkot erikoistyökurssin yritysverkon varmuuskopiointiratkaisuksi, sillä se on helppo ja nopea asentaa, sekä sen konfiguroiminen on melko mutkatonta. Lisäksi Flexbackup-ohjelma sopii hyvin pienille ja keskisuurille tietojärjestelmille, aivan kuten kurssin rakennettava yritysverkkokin on.

Ohjelman asennukseen liittyvät toimenpiteet, ohjelman konfigurointi ja käyttäminen käydään seuraavissa kappaleissa läpi yksityiskohtaisesti. Ohjeet ovat tehty melko yksinkertaiseksi, jotta jokainen kurssilla oleva osaisi hyödyntää niitä.

5.1 SSH-yhteyden konfigurointi

Flexbackup hyödyntää joko RSH- tai SSH-yhteyttä verkossa tapahtuvaan varmuuskopiointiin. Työssä käytetään SSH-yhteyttä muodostamaan yhteys varmuuskopiointiserveriltä asiakaskoneisiin. Kuitenkin SSH-yhteyttä muodostaessa asiakaskoneet kysyvät tyypillisesti aina salasanaa kirjautuessa asiakaskoneen järjestelmään. Tämä ominaisuutta emme kuitenkaan kaipaa Flexbackup-järjestelmässä, sillä tällöin olisi hankalaa suorittaa ajastettuja varmuuskopioita *(Tällöin kirjauduttaessa asiakaskoneelle varmuuskopiointiprosessin yhteydessä jouduttaisiin kirjoittamaan joka kerta salasana uudelleen).* Tämä voidaan ohittaa, tekemällä serverikoneella yleinen ja julkinen salausavain. Yleisen salausavaimen avulla voidaan kirjautua asiakaskoneelle ilman salasanan kyselyjä. Serverikoneen yleinen salausavain kopioidaan tiettyyn tiedostoon asiakaskoneelle, jolloin voidaan hyödyntää SSH-yhteyttä Flexbackup ohjelmassa. Tämän vuoksi voidaan tehdä omakäyttäjätunnus, jolle voidaan luoda omat avainparit, mutta tässä käytetään root käyttäjätunnusta. *(Yleensä ei ole suotavaa käyttää root-tunnusta, sillä se on tietoturvallisista syistä epäilyttävää. Kuitenkin tässä työssä se helpotti Flexbackup-ohjelman käyttöä, koska root käyttäjätunnuksilla on riittävät oikeudet kansioihin)*

Serverin (Office4) avainparin muodostaminen luodaan seuraavilla toimenpiteillä:

```
office4@lahi:~> su
password:                                    #SYÖTA SALASANA
```

```
office4@root:~> ssh-keygen -t rsa              #AVAINPARIN MUODOSTUSKOMENTO
Generating public/private rsa key pair.
Enter file in which to save the key (/root/.ssh/id_rsa):
Created directory '/root/.ssh/'.
Enter passphrase (empty for no passphrase):    #PAINA ENTER
Enter same passphrase again:                  #PAINA ENTER
Your identification has been saved in /root/.ssh/id_rsa.
Your public key has been saved in /root/.ssh/id_rsa.pub.
The key fingerprint is:
3e:4f:05:79:3a:9f:96:7c:3b:ad:e9:58:37:bc:37:e4 office4@root
```

(Koski & Kajala 2005, s.560)

Seuraavaksi kopioidaan avainparin julkinen osa (id_rsa.pub) kaikille niille asiakaskoneille, missä tätä avainparia halutaan hyödyntää. Tässä tapauksessa koneelle: Office5. Tässä vaiheessa on myös hyvä tarkistaa, onko asiakaskoneella jo kopioituna jonkun muun tietokoneen yleistä avainta kyseiseen tiedostoon. Jos yleistä avainta ei ole kopioitu, niin tällöin voidaan kopioida scp komennolla id_rsa.pub tiedosto Office5-koneen authorized_key2 tiedostoon.

```
scp /root/.ssh/id_rsa.pub  192.168.10.5:/root/.ssh/authorized_keys2
```

Tämän jälkeen voidaan kirjautua SSH:lla koneelta Office4 koneelle Office5 rootin tunnuksilla ilman salasanan kyselyjä. Korostan kuitenkin edelleen, että tyypillisesti tätä ei kannata tehdä root-tunnukselle.

5.2 Ohjelman asentaminen

Flexbackup-ohjelma tarvitsee toimiakseen tiettyjä tiedostoja ja ohjelmia. Seuraavassa on listattuna ne ohjelmat, joita Flexbackup tarvitsee tai hyödyntää:

- o perl
- o fileutils, findutils
- o dump/restore, afio, GNU tar, star, pax, cpio, zip (vaihtoehtoiset)
- o mt (käytettäessä nauhoja)
- o gzip, bzip2, lzop, or compress (vaihtoehtoiset)

o buffer (vaihtoehtoinen, tarvitaan yli 2 Gb tiedosotojen kääntämisessä)

(Flexbackup 2003)

Kuitenkaan Flexbackup-ohjelman peruskäyttöön Debian-järjestelmässä ei tarvitse asentaa kaikkia listalla olevia ohjelmia, sillä useimmat niistä ovat jo valmiina monissa UNIX-pohjaisissa järjestelmissä. Ohjelmassa hyödynnetään pääasiassa perliä sekä pakkausohjelmia. Kuitenkaan afio:ta, dump:ia eikä bufferia tarvita tässä käytössä, joten niitä ei asenneta.

Itse Flexbackup-ohjelman asentaminen voidaan suorittaa kolmella eri tapaa. Asennukset tehdään root-käyttäjätunnuksella. Helpoin tapa on asentaa ohjelma on käyttää komentoa: apt-get install flexbackup.

```
office4:/home/lahi# apt-get install flexbackup
```

Toisena tapana voidaan käyttää rpm-pakkausmanageriohjelmaa, jolla voidaan asentaa ja päivittää ohjelmia. Kuitenkin asennettava tiedosto on haettava tietokoneelle ensin Internetistä, sillä rpm ei tee sitä automaattisesti. Tiedosto voidaan hakea esimerkiksi osoitteesta:
http://www.flexbackup.org/RPMS/flexbackup-1.2.1-1.noarch.rpm

Tämän jälkeen siirrytään kansioon, missä rpm tiedosto sijaitsee ja itse asennus voidaan suorittaa komennolla:

```
office4:/# rpm –Uvh flexbackup-1.2.1-1.noarch.rpm
```

Tällöin rpm asentaa ohjelman automaattisesti, eikä käyttäjän tarvitse tehdä muuta.

Kolmas tapa asentaa Flexbackup-ohjelma on perinteinen lähdekoodista asentaminen. Ensin käyttäjän täytyy hakea itse ohjelma Internetistä, esimerkiksi osoitteesta:
http://www.flexbackup.org/tarball/flexbackup-1.2.1.tar.gz

Seuraavaksi siirrytään kansioon, missä tiedosto sijaitsee ja puretaan pakattu tiedosto, jonka jälkeen käännetään lähdekoodit ja asennetaan itse ohjelma:

```
tar xzvf flexbackup-1.2.1.tar.gz
make
make install
```

5.3 Ohjelman konfigurointi

Flexbackup-ohjelman konfigurointi perustuu flexbackup.conf tiedostoon, joka sijaitsee oletusarvoisesti hakemistossa /etc. Tiedoston avulla voidaan konfiguroida lähes kaikki toimenpiteet, jota ohjelma käyttää tai hyödyntää. Tiedoston sisältö on melko pitkä, jonka vuoksi seuraavassa on lueteltuna tärkeimpiä osia niistä, joita pitää tai kannattaa muuttaa, tai ovat muuten vain tärkeitä kohtia. Esimerkki konfiguraatiotiedostosta löytyy osoitteesta: http://www.flexbackup.org/flexbackup.conf.txt

```
# Varmuuskopion tyyppi. Voi olla: afio, dump, tar, cpio, star, pax, zip, lha,
# ar, shar
 $type = 'tar';

# Vakiovarmuuskopiosettien asetus, asetetaan hakemistot, mistä
# varmuuskopiot otetaan. Verkossa tapahtuvat varmuuskopiot määritellään IP-
# osoitteiden perusteella.
 $set{'office4-home'} = "/home";
 $set{'office5-home'} = "192.168.10.5:/home ";
# Kompressiointiohjelman valinta
 $compress = 'gzip';  # false/gzip/bzip2/lzop/zip/compress/hardware
 $compr_level = '4';  # Kompressointitaso (1-9) (for  gzip/bzip2/lzop/zip)

# Varmuuskopioiden säilytyspaikka
 $device = '/var/backups';

# Etäyhteyden valinta
 $remoteshell = 'ssh'; # (rsh/ssh/ssh2)

# Staattiset tiedostonnimet varmuuskopioissa, tällöin ei laiteta  päivämäärää
# tiedoston nimeen
 $staticfiles = 'false';

# Varmuuskopioista poisjätettävät tiedostot
$exclude_expr[0] = '.*/[Cc]ache/.*';
$exclude_expr[1] = '.*~$';
```

```
# Loki- ja aikaleimatiedostojen asetukset
logdir = '/var/log/flexbackup';       # Hakemisto lokeille
$comp_log = 'gzip';                   # Kompressointiloki false/gzip/
                                      # /bzip2/lzop/compress/zip
$staticlogs = 'false';                # Staattiset lokitiedoston nimet w/ no
                                      # date stamp
$prefix = '';                         # Lokitiedostot alkavat tällä
                                      # etuliitteellä
$stampdir = '/var/lib/flexbackup';    # Hakemisto varmuuskopioinnin
                                      # aikaleimoille
$keyfile = '00-index-key';            # Tiedoston nimi keyfile:lle jos
                                      # arkistoidaan hakemistoja
$sprefix = '';                        # Aikaleimojen tiedostot alkavat tällä
                                      # etuliitteellä
```

5.4 Ohjelman käyttäminen

Ohjelmaa ajetaan komennolla flexbackup, mutta varsinaiset toiminnot se saa parametrien avulla, jotka lisätään komennon loppuun viivan avulla. Flexbackupin komennoista saa tarkempaa tietoa komennolla flexbackup -help, joka näyttää kaikki komennot, joita ohjelmalla voidaan ajaa. Sama lista löytyy myös Internetistä osoitteesta: http://www.flexbackup.org/usage.txt

Ajettavia komentoja löytyy melko runsaasti, mutta seuraavassa on listattuna tärkeimpiä itse varmuuskopioimisesta, sen ajastamisesta, varmuuskopioiden listaamisesta ja lukemisesta sekä palauttamisesta ja muista komennoista:

VARMUUSKOPIOIMINEN:

```
flexbackup -dir <dir>           # Ottaa varmuuskopion halutusta kansiosta
flexbackup -dir otherhost:/usr  # Ottaa varmuuskopion toisen tietokoneen
                                # kansiosta
flexbackup -set all             # Ottaa varmuuskopion kaikista
                                # varmuuskopiosetteihin määritellyistä
                                # tiedostoista
flexbackup [...] -level <n>     # Varmuuskopiointi taso, voi olla numero tai
                                # full/differential/incremental
```

VARMUUSKOPIOIDEN AJASTAMINEN:

Flexbackup ohjelmassa on parametri, jonka avulla varmuuskopiointi voidaan ajaa jos viikonpäivä on sama kuin varmuuskopiointiin asetettu päivä. Päivä asetetaan numerolla, sunnuntait ovat 0 tai 7. Tätä komentoa voidaan hyödyntää esimerkiksi crontab:ssa. Komento ja sen parametri on:

```
flexbackup [...] -wday <n>
```

Varmuuskopiot voidaan ajastaa UNIX:ssa toimivan cron-ohjelman avulla, jolla voidaan ajastaa UNIX:ssa käynnistyviä ohjelmia. cron lukee ajastusohjeet crontab-ohjelman ajastustiedostosta. crontab sijaitsee /etc hakemistossa, ja sitä voidaan muokata tavallisella tekstieditorilla.

Seuraavassa yksinkertainen esimerkki crontab:iin lisättävästä tekstistä:

```
# Kotihakemistojen varmistus kello 3:31
# Päivittäiset inrementaaliset varmuuskopiot joka arkipäivä (catch day-to-
# day changes)
# Viikottaiset differentiaaliset varmuuskopioinnin lauantaisin (catch all
# changes since full)
# Täysi varmuuskopiointi – kerran kuukaudessa sunnuntaina
31   3    *     *  1-5 root flexbackup -set office4 -incremental
31   3    *     *    6 root flexbackup -set office4 -differential
31   3  1-7     *    * root flexbackup -wday 7 -set office4 -full -type afio
```

Crontabin toimintaperiaate:

```
# +---------------- minuutit (0 - 59)
# |  +------------- tunnit (0 - 23)
# |  |  +---------- kuukauden päivä (1 - 31)
# |  |  |  +------- kuukausi (1 - 12)
# |  |  |  |  +---- viikonpäivä (0 - 7) (sunnuntai = 0 tai 7)
# |  |  |  |  |
# *  *  *  *  *     komento,joka suoritetaan tulee tähän
```

VARMUUSKOPIOIDEN LISTAAMINEN JA LUKEMINEN:

```
flexbackup -list       # Listaa tiedostot varmuuskopiosta
flexbackup -compare    # Vertaa varmuuskopiotiedostoja
flexbackup -toc   # Listaa hakemiston, missä viimeisimmät varmuuskopiot ovat
flexbackup -toc all    # Listaa kaikki hakemistot, missä varmuuskopiota on
```

VARMUUSKOPIOIDEN PALAUTTAMINEN:

```
flexbackup –extract              # Purkaa kaikki varmuuskopiot hakemistoon,
                                 # missä käyttäjä on.
flexbackup -extract -flist <f>   # Purkaa ainoastaan ne varmuuskopiot, jotka
                                 # ovat listattuna <f> kohdassa hakemistoon,
                                 # missä käyttäjä on.
flexbackup -extract -onefile <f> # Purkaa yksittäisen varmuuskopion, mikä on
                                 # listattu kohdassa <f> hakemistoon, missä
                                 # käyttäjä on.
```

Oheisten käskyjen lisäksi varmuuskopioita voidaan palauttaa normaalilla tar-purku käskyllä. Komento voisi olla esimerkiksi:

```
tar xzvf purettavan_tiedoston_nimi.tar.gz /hakemisto/minne/puretaan
```

MUUT KOMENNOT:

```
flexbackup -version   # Näyttää käytössä olevan version Flexbackup-ohjelmasta
```

6 SKRIPTI-POHJAISEN VARMUUSKOPIOINTIOHJELMAN KONFIGUROINTI JA KÄYTTÄMINEN

Varmuuskopiointijärjestelmänä voidaan käyttää hyvinkin yksinkertaista ohjelmaa. Ohjelma voidaan ohjelmoida esimerkiksi UNIX:n shell-skriptiksi, joka käyttää UNIX:n käskyjä ja komentoja hyväkseen. Tällainen skripti-pohjainen ohjelma on erittäin helppo toteuttaa ja sen käyttäminen on myös vaivatonta. Scritptin asentamista ei yleensä tarvita.

Esimerkki tällaisesta hyvin yksinkertaisesta ohjelmasta on oma tekemäni skripti, joka hyödyntää SSH:n kopiointitoimintoa scp:tä sekä tar-pakkausmenetelmää. Ohjelmassa ensin kopioidaan Office5-koneelta /home hakemisto Office4-koneen /var/backups/temp hakemistoon, jonka jälkeen suoritetaan temp-hakemiston pakkausoperaatio ja versionhallinta. Lopuksi poistetaan kyseinen temp-hakemisto ja listataan /var/backups -hakemiston sisältö. Lisäksi skripti hyödyntää kappaleessa 5.1 SSH:n konfigurointi esiteltyä julkisen avaimen menetelmää. Ohjelma on tallennettu hakemistoon /var/backups nimellä backuppi.sh. Seuraavassa itse skripti:

```
#!/bin/sh

#Määritellään vakiohakemistot
BACKUPBASE="/var/backups"
SOURCEDIR="/home"
TEMP="/var/backups/temp"
CLIENT="192.168.10.5"

#Siirrytään varmuukopiointikansioon ja luodaan temppi
cd $BACKUPBASE
mkdir temp
cd temp

#Kopioidaan Office5 koneelta /home hakemisto temppiin
scp -r root@$CLIENT:$SOURCEDIR $TEMP

#Varmuuskopioinnin versionhallintaa.
mv $BACKUPBASE/Varmuuskopio.2.tgz $BACKUPBASE/Varmuuskopio.3.tgz 2> /dev/null
mv $BACKUPBASE/Varmuuskopio.1.tgz $BACKUPBASE/Varmuuskopio.2.tgz 2> /dev/null
mv $BACKUPBASE/Varmuuskopio.tgz $BACKUPBASE/Varmuuskopio.1.tgz 2> /dev/null
tar czvf $BACKUPBASE/Varmuuskopio.tgz $TEMP
```

```
#Lopuksi siirrytään varmuuskopiointikansioon ja tuhotaan temp hakemisto
cd $BACKUPBASE
rm -rf temp

#Tulostaa varmuuskopiointikansion sisällön
ls –hs

#OHJELMA PÄÄTTYY
```

6.1 Ohjelman konfigurointi

Skripti-pohjaisia ohjelmia on erittäin helppo konfiguroida ja muokata. Skriptien koodeihin on helppo lisätä omia toiminnallisuuksia ja käskyjä, jolloin ohjelmasta saadaan mieleinen ja omiin tarpeisiin sopiva kokonaisuus.

Tämän esimerkki-skriptin konfigurointi omiin tarpeisiin tapahtuu muokkaamalla koodin vakiomuuttujien BACKUPBASE, SOURCEDIR, TEMP ja CLIENT sisältöä.

```
BACKUPBASE="/var/backups"       # Hakemisto, johon varmuuskopiot tallennetaan
SOURCEDIR="/home"               # Asiakaskoneen hakemisto, mistä
                                # varmuuskopiot otetaan
TEMP="/var/backups/temp"        # Väliaikainen tiedosto, johon kopioidaan
                                # hetkeksi tiedostot asiakaskoneelta
CLIENT="192.168.10.5"           # Asiakaskoneen IP-osoite
```

6.2 Ohjelman käyttäminen

Kyseistä skripti-pohjaista varmuuskopiointiohjelmaa voidaan käyttää ajamalla se komennolla: ./var/backups/backuppi.sh. Tämän jälkeen ohjelma suorittaa halutun varmuuskopiointitoimenpiteen. Ohjelma voidaan myös ajastaa ottamaan täysiä varmuuskopioita UNIX:m crontab-työkalun avulla. Esimerkki crontab:iin kirjoitettavasta rivistä, joka ottaa täyden varmuuskopion joka arkipäivä kello 3:31 root-käyttäjätunnuksella:

```
31   3    *     *  1-5 root ./var/backups/backuppi.sh
```

7 YHTEENVETO JA JOHTOPÄÄTÖKSET

Harjoitustyön alkupuolella selvitettiin varmuuskopioinnin tärkeimpiä käsitteitä ja toimintoja. Selvityksistä kävi ilmi, että varmuuskopiointi ei ole itsestään selvyys, eikä sen tärkeyttä kannata missään tapauksessa vähätellä. Varmuuskopioinnin avulla voidaan ennalta ehkäistä suuriakin katastrofeja sekä ongelmia. Kuitenkin varmuuskopioita tulee ottaa riittävän usein, jotta niistä olisi tarvittaessa hyötyä.

Varmuuskopiointijärjestelmän käyttöönottoa kannattaa suunnitella tarkoin ja huolella. Tämän vuoksi järjestelmän käyttäjien ja sen ylläpitäjien tulee hallita ja osata hyvin varmuuskopioinnin perusperiaatteet sekä perusteet varmuuskopioinnista. Ennen järjestelmän käyttöönottamista tulee tietää tarkalleen, mitä ominaisuuksia ja toimintoja järjestelmältä halutaan, ja kuinka paljon sen omistajat ovat valmiita maksamaan kyseisestä järjestelmästä. Tietojen turvaamisesta ei kannata maksaa enempää kuin niiden arvo on.

Työn käytännön osuus puolestaan osoitti, että varmuuskopiointiohjelman asentaminen, konfigurointi ja käyttäminen eivät ole vaikeita operaatioita. Kuitenkin varsinkin varmuuskopiointiohjelmien asennuksessa ja konfiguroinnissa tulee kiinnittää erityistä huomiota huolellisuuteen ja annettuihin neuvoihin. Noudattamalla ohjelman manuaaleja ja ohjeita varmuuskopiointijärjestelmän rakentaminen ei yleensä pitäisi olla mikään ongelma. Lisäksi harjoitustyö osoitti myös sen, että oman varmuuskopiointiohjelman koodaaminen ja käyttäminen ei ole kovin vaikeaa.

LÄHTEET

Amanda 2007, The Advanced Maryland Automatic Network Disk Archiver, University of Maryland
http://www.amanda.org/
Viitattu: 9.2.2007

Durham J. 2002. Linux+ -sertifikaatti. Helsinki, IT Press. 597 s. ISBN 951-862-652-2

Flexbackup 2003, A flexible backup tool
http://www.flexbackup.org
Viitattu: 9.2.2007

Koski R. 2000. Linux MAN-sivut & järjestelmänhallinta. Jyväskylä, Gummerus. 690 s. ISBN 951-826-182-2

Koski R. ja Kajala T. 2005. Linux, ylläpitäjän käsikirja. Helsinki, Edita Prima Oy. 735 s. ISBN 951-826-733-2

Laitinen J. 2004, TL9133 Tiedonsiirtotekniikka 2
http://www.tekniikka.oamk.fi/~jyrkila/0405/tl9133/tl9133.kalvot.pdf
Viitattu: 9.2.2007

Linux About 2007 A, Linux / Unix Command: star
http://linux.about.com/library/cmd/blcmdl1_star.htm
Viitattu: 9.2.2007

Linux About 2007 B, Linux / Unix Command: pax
http://linux.about.com/library/cmd/blcmdl1_pax.htm
Viitattu: 9.2.2007

Linux About 2007 C Linux / Unix Command: zip
http://linux.about.com/od/commands/l/blcmdl1_zip.htm
Viitattu: 9.2.2007

Linux About 2007 D, Linux / Unix Command: awk
http://linux.about.com/b/a/136473.htm
Viitattu: 9.2.2007

Microsoft 2004, Varmuuskopioinnin perusteet
http://www.microsoft.com/finland/athome/security/update/backup.mspx
Viitattu: 9.2.2007

Safari Books 2006, OnlineComparing tar, cpio, and dump
http://safari5.bvdep.com/0596102461/I_0596102461_CHP_3_SECT_13#X2ludGVybmFsX1RvYz94bWxpZD0wNTk2MTAyNDYxL0lfMDU5NjEwMjQ2MV9DSFBfM19TRUNUXzEz
Viitattu: 9.2.2007