Examensarbete

HÖGSKOLAN I SKÖVDE

LAGRING AV SÄKERHETSKOPIOR PÅ MOLNBASERADE PLATTFORMAR

Jämförelse mellan molnbaserade plattformar för att lagra säkerhetskopior

Examensarbete inom huvudområdet Datalogi
Grundnivå 15 högskolepoäng
Vårtermin 2014

Jim Friberg

Handledare: Helen Pehrsson
Examinator: Jonas Mellin

Sammanfattning

Det finns flera olika sätt att säkerhetskopior, några vanliga sätt är lokal säkerhetskopiering, fjärrbaserad säkerhetskopiering och säkerhetskopiering som lagras på en molnplattform. Då det finns många leverantörer som erbjuder molnbaserade lösningar som gör det möjligt för en användare att lagra filer på respektive plattform kommer enbart molntjänsterna, ”Mega” och ”Dropbox for Business” att användas. För att besvara delfråga 1 utförs en litteraturstudie med tillhörande analys, för att besvara delfråga 2 och 3 kommer flertalet kvasiexperiment att utföras i en labbmiljö. Dropbox har en speciell avdelning som sysslar enbart med säkerhetsrelaterade frågor som förespråkar att AES med 256 bitars kryptering bör användas. Mega menar att 128 bitars AES kryptering räcker för att kryptera data då hårdvarubelastningen blir onödigt hög om starkare kryptering används.

Nyckelord: Backup, Molnlagring, jämförelsestudie, säkerhetskopiering, Windows.

Innehållsförteckning

1 Introduktion ... 1
2 Bakgrund ... 2
2.1 Användning av datormoln ... 2
2.2 Automatisering ... 3
2.3 Varför använda datormoln? ... 3
3 Problem ... 5
3.1 Problemprecisering ... 5
3.2 Motivering ... 5
3.3 Avgränsning ... 6
4 Metod ... 7
4.1 Analys baserad på litteraturstudie ... 7
4.2 Experiment ... 7
5 Tidigare forskning ... 11
6 Genomförande ... 12
6.1 Litteraturstudie ... 12
6.2 Experiment ... 12
6.2.1 Hårdvara ... 12
6.2.2 Mjukvara ... 13
6.2.3 Mätmetoder ... 14
7 Resultat ... 16
7.1 Litteraturstudie ... 16
7.1.1 Mega ... 16
7.1.2 Dropbox ... 17
7.2 Experiment ... 19
7.2.1 Total effektiv tid för skapandet och överförning ... 19
7.2.2 Total tid ... 20
7.2.3 Tid för skapandet av lokal säkerhetskopia ... 21
7.2.4 Tid för att föra över en säkerhetskopia ... 22
7.2.5 Tid för att ladda ner en säkerhetskopia ... 23
7.2.6 Jämförelse molnplattform och operativsystem ... 24
7.2.7 Automation och integration ... 25
8 Analys ... 26
8.1 Litteraturstudie ... 26
8.2 Experiment ... 26
9 Slutsats ... 29
9.1 Sammanfattning ... 29
9.2 Diskussion ... 30
9.3 Framtida studier ... 31

1 Introduktion

Säkerhetskopiering är en process för att skapa en kopia av delar av ett eller ett helt filsystem. Vid t.ex. ett eventuellt diskfel kan data återställas från säkerhetskopior till dess ursprungliga form från det att sista säkerhetskopian skapades. Det finns flera olika sätt att lagra dessa säkerhetskopior, några vanliga sätt är lokal säkerhetskopiering, fjärrbaserad säkerhetskopiering och säkerhetskopiering som lagras på en molnplattform. För att skapa säkerhetskopior och välja vad som skall ingå i dessa är två metoder vanliga, kontinuerlig säkerhetskopiering och inkrementell säkerhetskopiering. Den förstnämnda, kontinuerlig säkerhetskopiering, är enligt Hanavan (2007), en process för att automatiskt lagra senaste datamodifikationer, detta gör det möjligt att kunna återställa data från den senast sparade modifikationen, d.v.s. den senaste versionen av t.ex. en fil. Den andra, inkrementell säkerhetskopiering, är enligt Rouse (2010), en process som enbart säkerhetskopierar data som modifierats efter den senaste säkerhetskopieringen. Exempel, enligt Rouse (2010), är om en fullständig säkerhetskopiering gjorts på en måndag, tisdagens inkrementella säkerhetskopiering kommer enbart inkludera filer som modifierats efter måndagens säkerhetskopiering. Onsdagens inkrementella säkerhetskopiering kommer enbart inkludera de filer som modifierats efter tisdagens inkrementella säkerhetskopiering.

Enligt Techsoup Global (2012), väljer en stor mängd användare och systemadministratörer att lagra säkerhetskopior och information på molnbaserade plattformar, varav detta är ett intressant område. En studie gjord av Techsoup Global (2012), visar att organisationer runt om i världen är intresserade av molnbaserade lösningar och att många har till viss del redan implementerat molnbaserade lösningar i sina organisationer, många andra har också planer på att göra detta inom en snar framtid. Detta skapar nya utmaningar för utvecklare som har datormoln som utvecklingsområde då frågor som t.ex. säkerhet, prestanda, prioritering av data och schemaläggning framkommer. Detta är några frågor som kommer att adresseras i denna studie.

2 Bakgrund

Idag är en stor mängd organisationer och företag intresserade av system för att lagra säkerhetskopior till förmånliga priser, det finns idag flera olika varianter att välja på. En lagringsmetod som blivit populär på senare tid är en teknik som kallas onlinebaserad säkerhetskopiering (Engelska ”Cloud backup”).

En stor utmaning med lagring av data på en molnbaserad plattform är, enligt Sinanc & Sagiroglu (2013), främst säkerhetsrelaterade aspekter om hur personlig data i datormoln kan vara tillräckligt skyddad mot parter som inte skall ha åtkomst till dessa data. Enligt Pearson (2009), delas ofta en molnbaserad infrastruktur mellan flera olika organisationer eller företag, genom exempelvis virtualisering. Det är därför viktigt att personlig, konfidentiell och känslig data skyddas, och är separerade från varandra. Det är även viktigt, enligt Pearson (2009), att grundläggande säkerhetsmekanismer finns implementerade i olika steg när en molnbaserad plattform skall utvecklas, exempelvis säkra webbinloggningar, kryptering av data, säkra kommunikationssessioner. Speciellt viktigt är detta, enligt Pearson (2009), när informationen innehåller personlig identifierbar data, känslig information, användardata eller unika enheters identiteter. Detta kan leda till att skaparen av data kan spåras om en obehörig person får tillgång till dessa. Personlig information skall, enligt Pearson (2009), skyddas från dataförlust eller datastöld, exempel på att motverka detta är säkerhetsskydd, genom att förhindra obehörig åtkomst till data. Detta inkluderar även tillgång till hårdvara som data finns lagrad på. Ett annat exempel på att motverka datastöld är genom kryptering.

Patel, Patel, Chaudhari, Patel, & Prajapati (2012), menar att det viktigt att värdera data och prioritera vad som skall ingå i säkerhetskopior, då prestanda kan påverkas beroende på krypteringsalgoritmer som används, då krypteringsalgoritmer kräver olika mycket datorkraft. Patel, m.fl. (2012), menar också att utan att värdera betydelse av data kan enorma prestandaförluster inträffa, genom att t.ex. kryptera all data med samma krypteringsalgoritm kan det vara att föredra att känslig data krypteras med en stark krypteringsalgoritm, och mindre viktig data med en svagare krypteringsalgoritm.

Molnbaserad lagring av säkerhetskopior lagras på liknande sätt som traditionell lagring av säkerhetskopior, men istället för att lagra kopian på samma, eller en annan hårddisk skickas data över internet och lagras på en server i ett datacenter, som en leverantör har skapat och äger. Detta skyddar dataförluster som kan inträffa vid olyckor, som t.ex. brand, översvämning och jordbävning (Fisher, T. 2014).

2.1 Användning av datormoln

Då många användare, enligt Techsoup Global (2012), väljer att placera sina säkerhetskopior på en molnbaserad plattform innebär detta nya utmaningar som kan vara både till fördel, men också nackdel för utvecklingen av nya plattformar, detta med hänsyn till t.ex. säkerhet men också flexibilitet. Integritet är något som berörs på molnplattformar, detta är i sin korthet förhindrande av obehörig access till data.

I en undersökning som gjordes av Techsoup Global (2012), tillfrågades 200 000 organisationer, vilka ingår i Techsoup Global Network, varav 10 500 svar återficks från organisationer i 88 olika länder. Värt att nämnas är att Techsoup Global inkluderar enbart ideella organisationer (icke vinstdrivande). I denna undersökning presenterades att 21 % av

de tillfrågade som redan använder sig redan av molnbaserade plattformar, använder sig av tekniken för att lagra säkerhetskopior. Detta inkluderar allt från säkerhetskopia av enstaka filer till lagring av katastrofåterställningar (d.v.s, en komplett säkerhetskopia av systemet). I samma undersökning ställdes frågan vilken molnbaserad applikation de troligtvis skulle vilja implementera i respektive organisation. Den applikation som flest organisationer skulle vilja implementera var fillagring och fildelning, detta bestod av 31 % av de tillfrågade. Applikationen som sedan var mest önskvärd var Email med 30 % och på tredje plats kom säkerhetskopiering och katastrofåterställning som bestod av 25 % av de tillfrågade. När denna undersökning gjordes hade 61 % av de tillfrågade redan implementerat ett eller flera molnbaseradesystem för att hantera säkerhetskopior (Techsoup Global, 2012). Med denna undersökning visas att intresset finns för molnbaserade plattformar och att kunna implementera en fungerande lösning för säkerhetskopiering och lagra dessa på en molnplattform är önskvärt.

2.2 Automatisering

Chang, Shams, Callas & Kern (2012), använder som argument till deras studie att en säkerhetskopiering skall kunna automatiseras. Exempelvis vore det kanske att föredra att schemalägga en säkerhetskopiering till att starta på natten istället för mitt på dagen då den blir näst intill obemärkt av andra användare. Med tanke på att när en molnplattform används kan denna vara olika belastad beroende vilka länder majoriteten av användarna kommer från, detta då tidszoner spelar roll. En molnplattform kanske inte är maximalt belastad när t.ex. Sverige har dag då användare från delar av USA har natt, detta kan göra det svårt att veta när det är optimalt att skapa ett säkerhetskopieringsschema. Som tidigare nämnts i denna rapport kan fjärrbaserad lagring användas för att skapa säkerhetskopior. Genom att använda en fjärrbaserad metod kan system utformas efter just individuell verksamhet. Detta är inte lika lätt när en molnbaserad plattform används, då många användare från många olika länder använder denna tjänst vid olika tidpunkter.

En process för att skapa en säkerhetskopia, eller återställa från en säkerhetskopia bör, enligt Chang, m.fl. (2012), ske inom ett rimligt tidsintervall, i kontrast till storlek på säkerhetskopian. Då säkerhetskopiering kan påverka andra delar och enheter i ett nätverk, exempelvis fördröjningar i nätverket som påverkar användare. Enligt Chang, m.fl. (2012), är det att föredra att kontrollera faktorer som kan påverka processen för säkerhetskopiering, exempelvis om kompression kan användas alternativt hur data krypteras.

2.3 Varför använda datormoln?

Traditionell lagring av säkerhetskopior som lagras utanför anläggningen, d.v.s. på en annan geografisk placering kostar ofta mycket pengar då denna lösning kräver ett sekundärt datacenter. Därför kan det vara värt att tänka över om en molnbaserad plattform istället kan användas. En fjärrbaserad lagring av säkerhetskopior kan beskrivas genom att en säkerhetskopia lagras på en annan server eller hårddisk än det primära systemet. En sådan kopia kan finnas placerad på ett helt annat geografiskt ställe vilket skyddar mot katastrofskadors som t.ex. översvämning, brand, jordbävning och liknande, dock kräver inte en molnbaserad lösning ett eget datacenter, utan kan t.ex. hyras av en extern part.

Att använda en molnplattform istället för en fjärrbaserad lagring kan vara kostnadseffektivt då många molnleverantörer erbjuder olika prisplaner beroende på hur mycket datautrymme kunden efterfrågar. Enligt Dropbox (2014d), får varje ny kund som använder Dropbox för företag 1000 GB att starta med när kontot skapas, varje användare som är länkad till respektive företagskonto får i sin tur 200 GB lagringsutrymme, det totala priset för ett konto baseras i sin tur på hur många användare som är länkade till detta konto. I och med att extra datautrymme kan anpassas efter antal användarkonton och antal anställda på ett företag, kan en molnbaserad lösning anpassas för att vara skalbar då extra datautrymme kan köpas till, alternativt nedgradera beroende på kundens behov.

Molnbaserade plattformar använder ofta Internet för koppla samman kundens nätverk med leverantörens, Internet är ett publikt datornätverk för att koppla samman flera datornätverk. Enligt Sundaresan, Donato, Feamster, Teixeira, Crawford & Pescap (2011), kan nätverksprestanda påverkas av flera olika faktorer, exempel på detta är genomströmning (engleska throughput), som i sin korthet beskrivs som genomströmningshastigheten av datapaket. En annan faktor, enligt Sundaresan, S. m.fl. (2011), är fördröjningar (engelska latency), vilket i sin korthet beskrivs som olika orsaker till att fördröjningar sker, exempelvis paketförluster, överbelastning på nätverket eller vid hög belastning på hårdvara. Värt att nämnas är att studien utförd av Sundaresan, S. m.fl. (2011), är riktad mot enheter som används av hemmaanvändare. Då företag också ofta använder sig av internetleverantörer för att få en fungerande internetanslutning påverkar dessa faktorer även nätverksprestanda i företagsnätverk. Skillnad kan dock finnas i enheter som används för företag, då företag ofta använder sig av betydligt mer komplexa tekniker och enheter för nätverk, exempelvis routrar som kan hantera större mängd datatrafik än vad en router för hemmabruk.

Genomströmning av datapaket och fördröjningar påverkar enligt, Sundaresan, S. m.fl. (2011) nätverksprestanda. Detta kan leda till flaskhalsar i system och nätverk, som i sin tur kan leda till konsekvenser som att t.ex. synkroniserade säkerhetskopior kan få ökade fördröjningar i nätverksöverföringar av data vilket påverkar nätverksprestanda. Detta tvingar systemadministratörer att söka efter alternativa lösningar, där en lösning kan vara att minska dataöverföringar med en osynkroniserad säkerhetskopia, vilket kan vara en ögonblicksavbildning (snapshot) som replikeras till molnplattformen. Skillnad på synkroniserad säkerhetskopia och osynkroniserad säkerhetskopia är främst att när en osynkroniserad säkerhetskopia sker, kan det primära systemet fortsätta att användas som vanligt utan att vänta på att säkerhetskopiering måste bli klar. I en synkroniserad säkerhetskopia måste systemet vänta på att denna process skall slutföras då den måste vara en exakt kopia av den primära sidan.

Tid är ett uttryck som ofta förekommer i resterande delar av denna rapport. Med tid menas, tid som det tar för att skapa säkerhetskopian och tid som det tar att föra över denna till molnplattformen. Dessa två är viktiga att skilja på.

3 Problem

3.1 Problemprecisering

Syftet med denna studie är att besvara följande fråga:

Hur skiljer sig lagring av säkerhetskopior på en molnbaserad plattform mot en NAS (Network attached storage)? Med avseende på prestanda, integration och integritet.

För att kunna besvara den övergripande frågan delas denna in i delfrågor. För att besvara den övergripande frågan är syftet att besvara följande delfrågor under arbetets gång:

1. *Hur data skyddas när den skickas*
2. *Hur hastigheten och tiden varierar för att skapa en säkerhetskopia samt göra en återställning från denna beroende på om en molnbaserad plattform eller en traditionell fjärrbaserad lagring används*
3. *Hur aktiviteten schemaläggs i systemet och hur diskret denna är för användare och systemadministratör*

Av dessa två delfrågor (1 och 2) har delfråga 2 högst prioritet och kommer att utföras först. Därefter kommer delfråga 1 att utföras. Delfråga 3 prioriteras lägst och skall utföras sist.

Som tidigare nämnts i denna studie bör en systemadministratör vara medveten om hur data skyddas när den blir tillgänglig på Internet, denna frågeställning är tanken att delfråga 1 skall besvara. Delfråga 2 skall besvara aspekter relaterade till åtkomsttid när en säkerhetskopia skapas, och skall sändas till en molnplattform. Åtkomsttid kommer att nämnas som prestanda i resterande delar av denna rapport. Detta för att få en uppfattning om hur lång tid det tar att nå en fil vid val av respektive molnplattform. Till sist beskrivs automation och integrering i systemet, d.v.s. transparens. Detta är tänkt att delfråga 3 skall besvara.

3.2 Motivering

Molnlagring är en metod som kan användas för att lagra säkerhetskopior online. På detta sätt kan lokal lagring undvikas och data kan istället lagras online och alltid vara tillgänglig. Molnbaserade lagringsmetoder har, enligt Techsoup Global (2012), blivit allt mer populärt att använda och därför har denna studie genomförts. Denna studie riktar sig till systemadministratörer som kan komma i kontakt med olika lagringsmetoder och system för att lagra säkerhetskopior. Att lagra säkerhetskopior på en molnbaserad plattform istället för att lagra dessa lokalt kan minska kostnader då många gånger ett externt företag äger IT-infrastrukturen, samt underlätta tillgängligheten då denna typ av datalagring enbart kräver en internetanslutning och en dator för att få tillgång till dessa säkerhetskopior. Det finns också andra aspekter som bör ses över när en molnbaserad lösning skall implementeras, exempel på detta är säkerhet, då data lagras på en IT-infrastruktur som ägs av en extern part, vilket gör att också denna part har tillgång till data som lagras på deras servrar.

3.3 Avgränsning

Då det finns många leverantörer som erbjuder molnbaserade lösningar som gör det möjligt för en användare att lagra filer på respektive plattform kommer enbart molntjänsterna, ”Mega v1.0.22” och ”Dropbox for Business v2.8.2 ” att användas. Molntjänsterna valdes ut med hänsyn till:

- Hur mycket gratis datautrymme som tjänsten erbjuder, Mega erbjuder 50 GB gratis, Dropbox for Business erbjuder 1 TB under en testperiod.
- Dropbox for Business använder sig av mjukvara riktad mot företag, för detta finns en testperiod som sträcker sig genom 14 dagar, denna testperiod är identisk med den kommersiella företagsversionen.
- Hur stora filer som kan laddas upp på plattformen, då säkerhetskopior kan vara kräva mycket utrymme skall det inte finnas några begränsningar på detta.
- Begränsningar i överföringshastigheten. Det skall helst inte finnas någon begränsning i överföringen gällande hastighet.

Dessa punkter är också argumenten till att just dessa två molnplattormar har valts, då de uppfyller alla dessa krav.

Detta arbete kommer enbart att fokusera på Windows system närmare bestämt Windows server 2008 R2 och Windows server 2012 R2. Windows valdes då många är bekanta med systemet och det används i stor utsträckning. Unixsystem skulle också behandlas i denna studie men pga. tidpress var inte detta möjligt att genomföra och därför gjordes avgränsningen att enbart Windows kommer att användas.

Arbetet kommer inte heller att behandla priser för molntjänster i större utsträckning då detta är något som kan komma att förändras hela tiden, men det spelar en viktig roll när en användare skall välja vilken molnplattform denna skall använda.

Studien är främst riktad mot systemadministratörer. Då detta är ett examensarbete i datalogi med inriktning nätverk och systemadministration.

Analys baserad på litteraturstudie för att behandla delfråga 1 kommer enbart att baseras på den information som går att hitta på Mega och Dropbox officiella hemsidor, detta då denna delfråga prioriteras lägre än delfråga 2, pga. tidsbrist har t.ex. inte protokollanalys genomförts.

Kontinuerlig och inkrementell säkerhetskopiering som nämns tidigare i denna rapport kommer inte att behandlas i denna studie, då genomförande och analys av detta inte är möjlig pga. den tidsram som är satt. Detta nämns istället som framtida studier i sektion 9.3.

4 Metod

4.1 Analys baserad på litteraturstudie

För att besvara delfråga 1 utförs en litteraturstudie med tillhörande analys, detta med hjälp av den information som tillhandahålls av respektive molntjänst. Detta för att kunna besvara vilka säkerhetsprotokoll som respektive molnleverantör erbjuder vid användning av deras plattform, samt hur deras användaravtal ser ut gällande lagring och användning av information. Då det kan vara svårt att mäta hur data skyddas när den skickas används en litteraturstudie för att jämföra de detaljer som tidigare nämnts. Detta genom att analysera användaravtal vilket är ett juridiskt bindande dokument och skall gå att lita på.

Validitet med hänsyn till litteraturstudie kommer att uppfyllas genom att använda pålitliga källor när det går. Med en pålitlig källa menas databaser som används i stor utsträckning inom vetenskapliga områden, några av dessa är ACM Portal och IEEE Xplore. Detta för att undvika att felaktig information används då vem som helst kan publicera innehåll på Internet vore det inte att föredra att använda slumpmässiga artiklar. Då information om vissa molntjänster inte kan nås genom vetenskapliga databaser måste information om dessa hittas, lämpligen på respektive molntjänsts officiella hemsida. Enligt Wohlin, Runeson, Höst, Ohlsson, Regnell, & Wesslén (2012), är det viktigt att vara medveten om att fakta kan ändras, därför är det viktigt att under arbetets gång kontinuerligt kontrollera användaravtal och källor, detta för att kontrollera att informationen är uppdaterad vid publicering, då dessa användaravtal är juridiskt bindande skall de gå att lita på utan att riskera validiteten. Ett hot mot validiteten är, enligt Wohlin, m.fl. (2012), att prioritera vilken fakta som skall användas då nyckelmålet med litteraturstudien är att studera relationer mellan orsaker och effekter. Om information samlas men inte påverkar effekten av experimentet, är denna information möjligtvis av mindre värde.

Alternativ metod som skulle vara möjlig att genomföra för att t.ex. bestämma vilka protokoll som används för att föra över data, är att använda mjukvara som t.ex. Wireshark för att samla upp datapaket som går via nätverkskortet, för att sedan analysera dessa och dess innehåll. På detta sätt kan t.ex. protokoll som används för att föra över data, men också protokoll som används för att kryptera data. Detta är dock inget som har gjorts i denna studie pga. den tidsram som var tillgänglig inte täckte detta, då det inte räcker med att samla in data, dessa data måste också analyseras. I denna studie används istället de användaravtal som finns att tillgå, och eftersom att dessa är juridiskt bindande skall de gå att lita på.

4.2 Experiment

För att besvara delfråga 2 och 3 kommer flertalet kvasiexperiment att utföras i en labbmiljö, kvasiexperiment används då testpersoner saknas. Då den övergripande frågeställningen inriktar sig på prestanda och funktionalitet kommer systemuppsättningar att göras för att kunna mäta resultat i en fysisk miljö. Genom att sätta upp fysisk miljö kommer det också vara möjligt att mäta tid för att skapa säkerhetskopior, samt den tid det tar att återställa från dessa. Detta är en stor del av detta arbete och stor vikt kommer att läggas på denna delfråga.

Delfråga 3 kommer att fokusera på möjlighet av schemaläggning samt hur diskret detta är för användare och systemadministratörer. Detta kommer att göras i samband med delfrågan ovan gällande hastighet.

För att testa hur dataöverföringar sker i en fysisk laborationsmiljö används fysiska servrar och kommersiella molnplattformar som är designade för företag och privatpersoner.

Detta för att få ut data som baseras på ett verkligt nätverk då det kan förekomma störningar och belastningar av olika typer, vilket inte kan fångas in av en litteraturstudie. Genom att använda ett experiment kan misstag reduceras, d.v.s. variabler som en litteraturkälla kanske inte tagit hänsyn till. Experiment genomförs då det i andra metoder kan vara svårt att framställa lika trovärdiga resultat, då mycket av informationen som finns om respektive molntjänst finns publicerad på respektive tillverkares hemsida. Det är inte säkert att resultat blir likvärdiga genom att enbart utföra en litteraturstudie, speciellt då inte all information går att hitta i kända databaser, utan istället på leverantörers hemsidor, vilket kan resultera i att information kanske baseras på en annan uppsättning hårdvara, samt att validiteten kan skilja sig beroendes på hur testen har genomförts.

Validitet är, enligt Wohlin, m.fl. (2012), viktigt att uppfylla. För detta identifierar och beskriver Wohlin, m.fl. (2012) flera hot mot validiteten. Ett hot, enligt Wohlin, m.fl. (2012), som kan påverka validiteten är låg statistisk styrka, detta hot beskriver förmågan att påvisa ett korrekt mönster i data. Molntjänsterna som används i denna studie är skapade av människor, vilket inte bör resultera i signifikanta avikelser mellan olika testkörningar. Skulle större avikelser förekomma finns det risk att något har påverkat resultatet.

Ett annat hot, enligt Wohlin, m.fl. (2012), är att aktivt söka efter ett önskvärt resultat, d.v.s. fiska efter ett önskvärt resultat. Detta är ett hot då om detta skulle ske är inte längre analysen oberoende och den person som utfört experiment kan påverka resultat genom att aktivt söka efter ett specifikt resultat. För att behandla detta hot har inget förväntat resultat gjorts i denna studie, d.v.s. personen som har utfört experiment har inte någon teori om vilken molnplattform som presterar bäst. Att inte ha någon teori om vilken molnplattform som presterar bäst minskar risken för att manipulera resultat så att förväntat resultat stämmer överens med det slutgiltiga resultatet. Likvärdiga tester utförs oberoende vilken molnplattform som testas utan att ändra variabler, detta minskar risken att manipulera mätmetoder och på detta sätt påverka resultat.

Pålitlighet eller reliabilitet av mått är, enligt Wohlin, m.fl. (2012), ett hot. Detta kan bero på många olika faktorer, exempel på dessa faktorer är bristfällig frågeställning eller bristfälliga mätverktyg. Den grundläggande principen för att behandla detta hot, är enligt Wohlin, m.fl. (2012), att när ett fenomen mäts flertalet gånger skall resultaten bli likvärdiga. Detta behandlas genom att utföra likvärdiga tester flera gånger för respektive molnplattform, skulle resultat vara likvärdiga varandra kan resultatet betraktas som pålitligt.

Wohlin, m.fl. (2012) beskriver slumpmässig irrelevans i experimentell uppsättning som ett hot. Detta hot beskriver externa händelser som inte är en del av den experimentella miljön, exempelvis ett plötsligt avbrott i experimentet. För att behandla detta hot har onödiga tjänster som kräver hårdvaruresurser och nätverkskapacitet stängts av i så stor utsträckning som möjligt, t.ex. automatiska uppdateringar. Detta är också ett sätt att hantera yttre påverkan, då denna studie kräver att en aktiv internetuppkoppling finns tillgänglig för att ansluta till respektive molnplattform, finns viss risk att yttre påverkan kan påverka resultat.

Detta är dock oundvikligt att helt kringgå då internetuppkoppling är ett krav när en säkerhetskopia skall skickas till molnplattformen. Genom att stänga av tjänster och program som inte är nödvändiga för att genomföra experiment hanteras yttre påverkan i så stor

utsträckning som möjligt, som tidigare nämnts måste en viss internetanslutning finnas tillgänglig för att skicka data till respektive molnplattform, finns inte möjligheten att helt eliminera yttre påverkningar.

Enligt Wohlin, m.fl. (2012), är validitet med hänsyn till konstruktion ett sätt att generalisera resultat av experiment till den teori som finns till grund bakom, detta hot relaterar till den experimentella designen och förmåga att studera denna design. Exempel på detta är, enligt Wohlin, m.fl. (2012), otillräcklig förklaring av konstruktionen, med detta menas att konstruktionen inte är tillräckligt definierad innan mått och behandlingar för att hantera denna konstruktion är komplett. Detta resulterar i att då teorin inte är tillräckligt tydlig, kan inte heller experimentet bli tillräckligt tydlig. Det är därför enligt Wohlin, m.fl. (2012), viktigt att definiera de begrepp och uttryck som används i studien för att dessa skall vara tydliga.

Hot mot den externa validiteten är, enligt Wohlin, m.fl. (2012), tillstånd som begränsar förmågan att generalisera resultat av experiment i en industriell tillämpning. Det finns tre olika interaktioner detta involverar: människor, plats och tid. I denna studie är de två sistnämnda relevanta då människor inte involveras i denna studie. Wohlin, m.fl. (2012) menar att ett hot är interaktion av uppsättning och behandling, med detta menas att när resultat skall generaliseras med hänsyn till en industriell tillämpning är det av vikt att använda representativ utrustning, d.v.s. likvärdig utrustning som skulle användas i verkligt scenario. Utifrån exempel som Wohlin, m.fl. (2012) beskriver, kan detta vara att använda utdaterade verktyg i ett experiment, detta är direkt olämpligt då uppdaterade verktyg skulle användas i ett verkligt scenario. Varav också detta tillämpats i denna studie, för att motverka hotet som Wohlin, m.fl. (2012) beskriver används enbart de senaste och stabila versioner av mjukvara som respektive molnplattform erbjuder, dessa är enligt Mega (2014d), Mega 1.0.22, och enligt Dropbox (2014a), Dropbox 2.8.3. De mätverktyg som används för att övervaka prestanda används standardversioner som finns förinstallerat på respektive operativsystem:

Windows server 2008 R2 (V6.1, build 7601 service pack 1) – Performance Monitor 6.1.7601.
Windows server 2012 R2 (V6.3, build 9600) - Performance Monitor 6.3.9600.

Dessa versioner kan jämföras med de som skulle användas i ett verkligt scenario då samtliga är standardversioner för respektive operativsystem. Respektive operativsystem är senast stabila byggnad när studien genomfördes.

För att generalisera extern validitet behandlas också, enligt Wohlin, m.fl. (2012), interaktion av historia och behandling, detta är den effekt av experimentet som genomförs vid en speciell tid på dygnet vilket kan påverka resultatet. För att behandla detta hot har ingen plan skapats för när respektive test skall utföras, genom att utföra tester oberoende tid på dygnet behandlas hotet som Wohlin, m.fl. (2012) identifierat angående tid när experiment utförs.

Alternativ metod som skulle vara möjlig är att intervjua personer som tidigare använt dessa molnplattformar, vilket kan ge en överblick om hur respektive molntjänst fungerar rent praktiskt med hänsyn till prestanda, säkerhet och integritet. Detta kan ge en allmän överblick om hur respektive person uppfattar tjänsten, vad som fungerat bra, vad som fungerat mindre bra.

Genom att använda denna metod kan automatiseringen av respektive molnplattform lätt utvärderas då det är personer som faktiskt jobbat praktiskt med plattformen och kan beskriva hur det fungerar rent praktiskt. Genom att använda denna metod kan det vara

problematiskt att inhämta rådata och sammanställa dessa och detta är också anledningen till att inte denna metod har används, då delmål 2 kan bli svårt att besvara.

5 Tidigare forskning

Det finns relativt få publicerade artiklar som behandlar prestandatester för säkerhetskopiering och hur dessa kopior lagras. Ett urval av de som finns behandlar främst säkerhetskopiering inom ett lokalt nätverk, vilket kan vara svårt att använda i denna studie då en markant skillnad finns mellan ett LAN och WAN, med hänsyn på nätverkshastighet.

Traeger, Joukov, Sipek & Zadok (2006), undersökte hur gratis webblagring kan användas för säkerhetskopiering, denna studie behandlar mindre filer (25 – 100 MB) än vad denna studie gör. De system som används i Traeger (2006), använder Gmail, GMX FreeMail, Hotmail, Sezna och Yahoo! Mail. Denna studie kommer fram till att gratis webblagring kan användas effektivt för att lagra säkerhetskopior vid mindre företag eller hemanvändare.

Johansson (2013), undersökte hur vanligt det är att användare använder någon form av säkerhetskopiering. Denna studie är genomförd via en enkätundersökning. Den behandlar också varför inte personer använder sig av någon form av säkerhetskopiering. Efter det att denna undersökning genomförts, menar Johansson (2013), att mer än hälften av de tillfrågade använder sig av någon form av lösning för att behandla säkerhetskopior. Baserat på svaren visade det sig också att flera personer aktivt har valt inte använda sig utav säkerhetskopior. För de som inte använder sig av en säkerhetskopiering var den främsta anledningen att det var svårt att automatisera dessa aktiviteter, samt att det kostade pengar.

6 Genomförande

Detta kapitel behandlar hur studien har genomförts. Som tidigare nämnts har en litteraturstudie använts och kvasiexperiment utförts, varav detta kapitel är indelat i litteraturstudie och experiment.

6.1 Litteraturstudie

För att behandla delfråga 1 (*Hur skyddas data när den skickas?*) har främst officiell dokumentation använts för respektive tjänst. Detta genom att läsa användaravtal som finns på hemsidan för respektive tjänst.

För att hitta information har sökmotorn Google Scholar använts samt databaserna ACM Digital Library och IEEE Xplore.

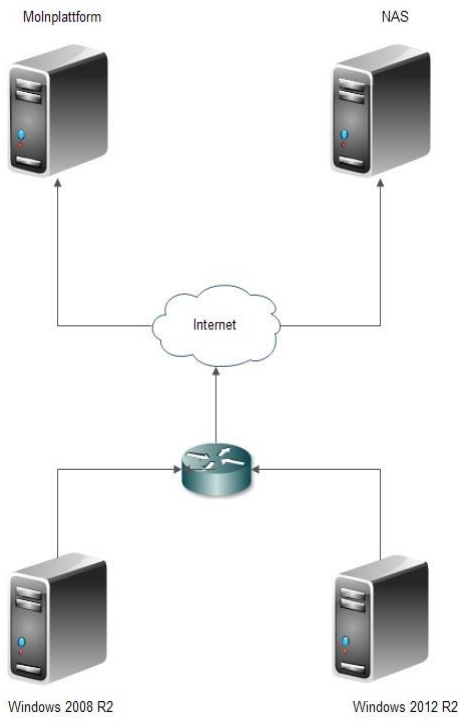
6.2 Experiment

6.2.1 Hårdvara

Den fysiska laborationsmiljön består av 3 stycken servrar och en router med internetuppkoppling. Resurser på dessa servrar är följande:

- Intel Core 2 CPU 6400 Processor med 2x 2,13 GHz klockfrekvens
- 4,00 GB RAM-minne, DDR2, 667 MHz
- Western Digital (WD1600AAJS-55B4A0) hårddisk. 150 GB, 7200 RPM
- Intel 82566DM Gigabit Network (10/100/1000 Mbit)
- Säkerhetskopia storlek – 13,9 GB (samma i varje test oberoende system)

Nätverkstopologi:



För att behandla den experimentella designen nämner, Wohlin, m.fl. (2012), olika principer om hur ett experiment kan designas, dessa är: ”slumpmässigt”, ”blockering” och ”balansering”. Då denna studie behandlar diverse tester vid olika tidpunkter och dagar kommer den slumpmässiga designen att användas, detta för att t.ex. prestandaförluster, resursutnyttjanden och liknande, på det interna eller externa nätverket vid just tidpunkten då testet utfördes vilket annars kan ha en inverkan på resultatet, detta nämns även under kapitel 4.1.2 Experiment. Denna studie kommer också att använda balansprincipen, detta då flera tester kommer att utföras för att bekräfta validiteten. Skulle enbart ett test utföras för respektive lösning kan det bli svårt att analysera resultat, då t.ex. prestandaförlust eller andra faktorer kan ha en viss inverkan på resultatet, detta behandlas i en sådan stor utsträckning som möjligt, genom att stänga av onödiga tjänster och liknande som tidigare nämnts i denna rapport (4.1.2 Experiment), då experiment behöver en aktiv internetuppkoppling mot varje molnplattform, finns ändå risk för att viss inverkan på den experimentella designen. Av denna anledning görs tre tester mot varje lagringsplattform. D.v.s. en balansdesign används då flera tester utförs och samma faktorer mäts för varje test och block. Dessa steg är viktiga för att kunna påverka validiteten positivt då genom att göra test som mäter samma saker flera gånger för att kunna bestämma om något externt har påverkat resultatet i större utsträckning. Resultaten kommer att presenteras i sin helhet, d.v.s. varje test kommer att presenteras i denna studie. Wohlin, m.fl. (2012), menar att efter det att data har samlats efter respektive test, är det viktigt att validera dessa data. Den första metod som nämns, är att kontrollera att data är fysiskt möjliga, d.v.s. att värden är logiskt möjliga, skulle detta inte vara fallet, har antagligen en extern påverkan haft för stor inverkan på resultatet, alternativt fel variabel har mätts, skulle detta inträffa kan validitet inte längre garanteras. Det är också enligt Wohlin, m.fl. (2012), viktigt att bestämma oberoende och beroende variabler. Då denna studies främsta fokus ligger på prestanda, är det av vikt att storleken på det som skall säkerhetskopieras är detsamma på alla system, annars kan resultat påverkas markant, om skillnad på säkerhetskopior skulle skilja. Detta då det tar längre tid att ladda ner eller upp ju större storleken på dessa är varav detta är en beroende variabel nämligen filstorleken.

6.2.2 Mjukvara

För att kunna jämföra prestanda på olika operativsystem används:

Windows server 2008 R2 (V6.1, build 7601 service pack 1) – Performance Monitor 6.1.7601.
Windows server 2012 R2 (V6.3, build 9600) - Performance Monitor 6.3.9600.

Detta då Windows server 2008 R2 är vanligt att använda, och Windows server 2012 R2 då detta är den senaste utgåvan av Windows server från Microsoft. Båda är standardutgåvan av Windows server med tjänsterna DHCP, DNS, Active Directory, ett antal delade mappar med innehåll och ”Windows server backup” installerat, utöver dessa tjänster finns också Dropbox och Megas synkroniseringsverktyg installerat på systemet (Mega v1.0.22 respektive ”Dropbox for Business v2.8.2).

För att mäta prestanda testas detta genom åtkomsttid, det vill säga den tid det tar att ladda upp eller ner en eller flera filer till respektive molnplattform. För att mäta detta kommer ett verktyg som finns inbyggt i Windows Server att användas. Detta program heter Prestandaövervakaren och används för att undersöka hur prestandan påverkas av program och tjänster som körs på systemet. Dessa data analyseras sedan.

Då test utförs för respektive molnplattform på både Windows server 2008 R2 och Windows server 2012 R2, används också samma version av prestandaövervakaren, beroende på om 2008 används eller 2012 (2008 – Performance Monitor 6.1.76.01 respektive 2012 - Performance Monitor 6.3.9600).

6.2.3 Mätmetoder

Som tidigare nämnts i denna studie är det viktigt att hålla isär tid som det tar att skapa säkerhetskopian lokalt på systemet och hur lång tid det tar att transportera denna till molnplattformen.

För att mäta hur lång tid det tar att skapa en säkerhetskopia lokalt på systemet används det inbyggda verktyget ”Event Viewer” som används för att logga händelser i Windows. I detta verktyg finns möjlighet att filtrera ut enbart händelser som är kopplade till Windows server backup och i denna finns datumstämplar när en säkerhetskopiering startar och avslutas. Detta kontrolleras också genom tidsstämplat i rådata som presenteras senare i denna rapport där processorbelastning kan utläsas. På detta sätt behandlas tid med hänsyn till lokal säkerhetskopiering.

För att hantera den tid det tar att transportera en säkerhetskopia lokalt på systemet till molnplattformen finns det två olika varianter. Den första genom att kontrollera händelseloggen på respektive molnplattform, vilket finns tillgängligt i de utvalda molntjänsterna. Den andra genom att kontrollera tiden när överföringarna startas till det att dessa finns lagrade på molnplattformen manuellt. För att validitet skall uppnås, kommer bägge varianter att göras i denna studie, detta för att kontrollera att dessa överensstämmer med varandra. Den sistnämnda metoden (andra) kommer att användas för att mäta den tid det tar att skicka säkerhetskopian till NAS systemet.

Den totala tiden är den tid det tar att starta en process kopplat till skapandet av en säkerhetskopia till det att denna är överförd till molnplattformen. Detta sker genom att manuellt kontrollera hur lång tid det tar från dess att processen startas till det att säkerhetskopian kan nås på molnplattformen. Detta för att kontrollera om det finns några större fördröjningar mellan det att säkerhetskopian skapats lokalt till det att den går att nå på molnplattformen.

För att kontrollera återställningstiden kontrolleras först den tid det tar att ladda ner diskavbilden från molnplattformen till en dator. Detta då en säkerhetskopia inte kan återställas direkt från molnplattformen utan måste först laddas ner till en externkälla som en användare sedan återställer från. Värt att nämnas är att den tid det tar att leta reda på säkerhetskopian och klicka sig genom menyer inte kommer att inkluderas i denna tid utan denna tid tar enbart hänsyn till själva återställningstiden som systemet använder. Detta då validiteten inte skall påverkas då det kan ta olika lång tid att skriva in kommandon och klicka sig vidare beroende på användarens hastighet.

För att kontrollera prestanda när data skickas till molnplattformen är detta möjligt genom att använda resurshanteraren i Windows (engelska ”Perfmon”). På detta sätt kan resultat presenteras genom grafer. I detta verktyg kan också schemaläggning göras vilket möjliggör att mätningen startar när en säkerhetskopiering startas till dess att den är klar. Det är också möjligt att välja vad som skall övervakas vilket passar bra till denna mätning då det är viss data som skall användas i resultatet.

En mall skapas för mätintervall samt vilka parametrar som skall mätas. Detta då mätningen skall vara identisk på alla mätningar som sker på alla maskiner.

Då det kan vara svårt att mäta automation kommer enbart en redogörelse att göras för att behandla denna del. Testerna kommer att schemaläggas för att utföras vid en specifik tidpunkt för att kontrollera möjligheten att integrera schemaläggning och få detta att fungera tillsammans med respektive lösning för att skapa en säkerhetskopia. Denna del kommer också att behandla integration som synkroniseringsverktygen har med systemet. Då båda molntjänster använder sig av synkroniseringsverktyg för att ladda upp filer på molnplattformen kommer dessa att laddas ner och installeras för att jämföra hur resurskrävande dessa är.

7 Resultat

Under följande kapitel kommer resultat från litteraturstudien att presenteras. Resultat från tester kommer också att presenteras. Experimentet har gjorts på datorer med Windows Server 2008 R2 respektive Windows Server 2012 R2. Alla tider mäts i sekunder för att få ett mer exakt resultat än vad minuter ger.

7.1 Litteraturstudie

Under följande kapitel kommer delfråga 1 att besvaras. I detta inkluderas t.ex. hur data skyddas när den skickas, hur respektive molntjänst ansvarar för dataförlust eller inte och hantering av nyckelhantering vid kryptering. Analys av litteraturstudie har begränsats till att enbart information som finns tillgänglig på respektive leverantörs hemsida kommer att behandlas, då denna delfråga prioriteras lägre än delfråga 2, (Se kapitel 7.2 Experiment).

7.1.1 Mega

Enligt Mega (2014a), ansvarar inte Mega för dataförlust. Detta kan göra det svårt för användare att återskapa filer som tagits bort. Detta är alltså, enligt Mega (2014a), inget kunden skall räkna med, dock finns chansen att data kan återskapas inom maximalt 30 dagar från det att datan togs bort från plattformen. Detta finns det dock, enligt mega (2014a), inga garantier för att data kan återskapas, varav detta inte heller är något som de erbjuder sina kunder.

En risk finns att data försvinner på plattformen vid t.ex. en diskkrasch eller likande, detta är något Mega inte tar ansvar och användare rekommenderas att lagra data som är kritisk på externa platser som kan garantera att data finns kvar. Detta gäller också vid borttagning av konton. Då skall användaren räkna med att datan också tas bort, också här finns möjligheten om användaren har tur att återställa data inom 30 dagar från det att kontot stängs av att återställa data. Detta är dock inget användaren skall räkna med. En användare äger, enligt Mega (2014b), sin egen krypteringsnyckel och genererar denna själv lokalt på datorn, denna nyckel skall, enligt Mega (2014b), hållas privat, detta för att inga externa parter skall få tillgång till denna och på det sätt få tillgång till datan som lagras på användarens Megakonto. Denna nyckel kan delas med andra parter om t.ex. filer skall delas med andra personer, eller om krypteringsnyckeln skrivs ner och sedan försvinner. Detta är en handling som Mega inte tar ansvar för, utan kunden genererar själv en krypteringsnyckel, som gör att filerna krypteras på plattformen det är sedan användarens eget ansvar hur denna hanteras.

All kryptering sker, enligt Mega (2014b), punkt till punkt, d.v.s. krypteringen sker genom hela sändningsförfarandet. Data som skall laddas upp på plattformen krypteras på enheten innan den skickas över Internet, data som skall laddas ner från plattformen dekrypteras först efter det att enheten har laddat ner data. Enheten som använder Megas plattform har, enligt Mega (2014b), ansvaret att generera, byta och hantera krypteringsnycklar, på detta sätt kommer aldrig en krypteringsnyckel lämna den lokala datorn, utom undantaget för publika nycklar som RSA algoritmen använder sig av. Dock krypteras enbart fil-data, filer, mappar och namn på dessa. Saker som E-mail adress, IP-adresser, mappstrukturer, ägarrättigheter och betalningsplan inkluderas inte, enligt Mega (2014c), i denna krypteringsprocess. Detta då ägarna av molnplattformen Mega ska ha möjlighet att spåra aktiviteter och användare som använder molnplattformen.

Tekniken som hanterar nycklar är enligt, Mega (2014c), baserad på öppen källkod, vilket innebär att en användare själv kan skriva program för att komma åt plattformen utan att använda de färdiga program som redan finns för synkronisering, detta verktyg finns enbart för Windows när studien gjordes, enligt Mega (2014) är också en lösning under utveckling för Mac och Linux.

För att överföra en säkerhetskopia med hjälp av synkroniseringsverktyget som finns för Windows skyddas data, enligt Mega (2014c), med AES-128 kryptering. Anledning till att inte AES-192 eller AES-256 används beror på att dessa två tekniker använder, enligt Mega (2014c) mer processorprestanda än vad AES-128 gör. Enligt Mega (2014c) är inte den teoretiska säkerhet som AES-192 och AES-256 bidrar med värd att implementera, då processorprestandan blir lidande. Även SSL och TLS används, enligt Mega (2014c), för att skapa säkra kommunikationstunnlar.

7.1.2 Dropbox

Som standard, enligt Dropbox (2014b), sparar Dropbox loggar och borttagna filer och gör det möjligt för en användare att själv återskapa filer. Dropbox säkerhetsdokument (Dropbox, 2014b) behandlar hur data behålls eller inte vid borttagning av konton, d.v.s. data finns kvar så länge kontot är aktivt eller en användare själv tar bort datan. Skulle ett konto tas bort kommer också, enligt Dropbox (2014b), data som tillhör detta kontot att tas bort. Enligt Dropbox (2014b), finns också möjlighet att kontrollera när t.ex. nya enheter ansluter till kontot, detta för att minska risken för att enheter som inte skall ha tillgång till kontot ansluter sig.

Enligt Dropbox (2014b), har de själva hand om krypteringsnycklar. Anledning till detta är att många funktioner kräver denna hantering då ett konto skall gå att nå från olika enheter och delning av mappar. Det skulle, enligt Dropbox (2014b), nästan vara omöjligt att erbjuda om alla användare att själva hantera dessa krypteringsnycklar. Möjligheten finns dock enligt Dropbox att själv hantera sina egna nycklar för att skapa egna krypteringsmetoder med andra produkter som t.ex. Bitlocker.

Enligt Dropbox (2014b), rekommenderas att välja ett starkt lösenord, då det minskar risken att obehöriga personer skall få tillgång till kontot. Skulle ett lätt lösenord användas, som en person lätt kan hitta, kan de filer som finns på kontot laddas ner direkt och datan kan inte längre behandlas som säker. Dropbox har utvecklat ett verktyg som användare kan använda för att testa om lösenordet betraktas som säkert. För att kryptera lösenord och http trafik till Dropbox-plattformen används HTTPS när kontot skall nås genom en webbläsare. En annan teknik, enligt Dropbox (2014b), för att påverka säkerhet positivt erbjuder också Dropbox en tjänst som kallas två-stegs, detta är enligt Dropbox (2014b) en metod att verifiera sin identitet dels via lösenord, men också en sexsiffrig kod för att logga in på en ny dator eller telefon. Detta för att användaren skall vara den person som den uppger sig att vara. Det finns också, enligt Dropbox (2014b), möjlighet att använda en händelsesida där en användare kan kontrollera kontoaktiviteter och information som t.ex. enheter som är och har varit anslutna till kontot under den senaste tiden. Det finns också möjlighet att övervaka vilka filer som används inom en viss tidsepok där en användare kan se vilka filer som öppnats eller laddats ner och upp.

Enligt Dropbox (2014b), är säkerhet en hög prioritet. För att överföra en säkerhetskopia med synkroniseringsverktyget används AES-256 bitars kryptering och för att föra över data säkert används SSL och TLS för att skapa säkra kommunikationstunnlar.

När en användare använder sig av tjänsten Dropbox finns möjligheten att använda sig av TOTP algoritmen (Time-based One-time Password Algoritm). Enligt Machani, M'Raihi, Pei & Rydell (2011), är detta en algoritm som räknar ut en engångslösenord från en delad hemlig nyckel och nuvarande tid. För att skicka säkerhetskopian till molnplattformen med hjälp av synkroniseringsverktyget som finns för Windows skyddas data med AES-256 kryptering. SSL och TLS används också för att skapa säkra kommunikationstunnlar.

7.2 Experiment

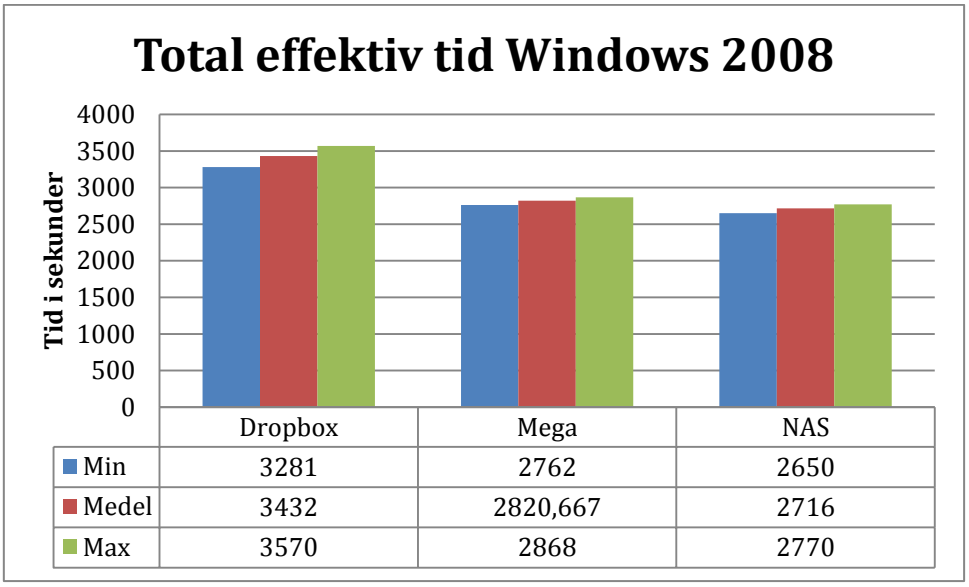
Under detta kapitel presenteras resultat för hur lång tid det tar att kopiera en säkerhetskopia till respektive molnplattform (Dropbox och mega) men också till en NAS. Då säkerhetskopior inte kan sparas direkt på molnplattformen genom verktygen ”Windows server backup” skapas säkerhetskopior lokalt på de olika system för att skicka dessa säkerhetskopior till respektive molnplattform med hjälp av synkroniseringsverktyg som erbjuds av Mega och Dropbox. Varje test utförs totalt tre gånger, varav medelvärde, maxvärde och minimumvärde för samtliga test presenteras i tabeller nedan, d.v.s. tre olika tester utförs för varje molnplattform och NAS på respektive operativsystem. Skulle en markant skillnad visa sig i resultat kan ett hot som adresserats tidigare i denna rapport inträffat, d.v.s. hot enligt Wohlin, m.fl. (2012), slumpmässig irrelevans i experimentell uppsättning, med detta menas att en extern variabel har påverkat resultatet.

För att mäta tiden det tar att kopiera en säkerhetskopia till respektive plattform görs detta genom att kopiera en säkerhetskopia från Windows Server 2008 R2 till Mega, Dropbox och NAS och likadant för Windows Server 2012 R2. För varje operativsystem och tjänst gjordes totalt 3 tester (Y-axeln anger test), tiden som det tog att slutföra testet (X-axeln anger tid). Storlek på säkerhetskopia - 13,9 GB.

7.2.1 Total effektiv tid för skapandet och överförning

I första testet som gjordes som kan ses i figur 7.1 och 7.2 , är den totala effektiva tiden som det tog att skapa en säkerhetskopia lokalt på datorn, samt hur lång överföringstid dessa hade, d.v.s. ladda upp säkerhetskopian till molnplattformen, detta test inkluderar dock inte väntetid mellan skapandet av säkerhetskopian och överföring utan enbart effektiv tid att skapa eller transportera säkerhetskopian (detta kommer att redovisas i sektion 7.2.2).

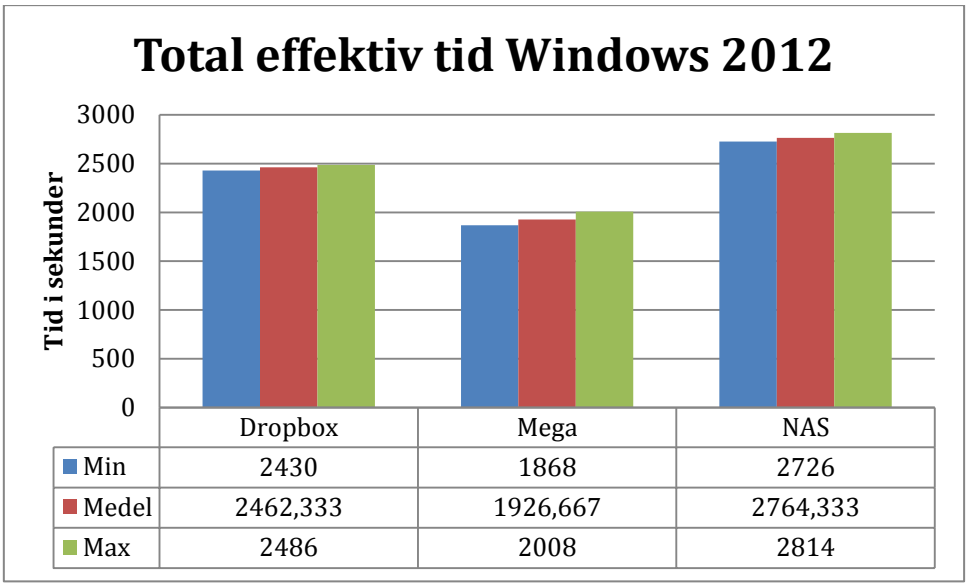
Windows Server 2008 R2



	Dropbox	Mega	NAS
Min	3281	2762	2650
Medel	3432	2820,667	2716
Max	3570	2868	2770

Figur 7.1 – Tid för skapandet av lokal säkerhetskopia samt överförning av denna.

Windows Server 2012 R2

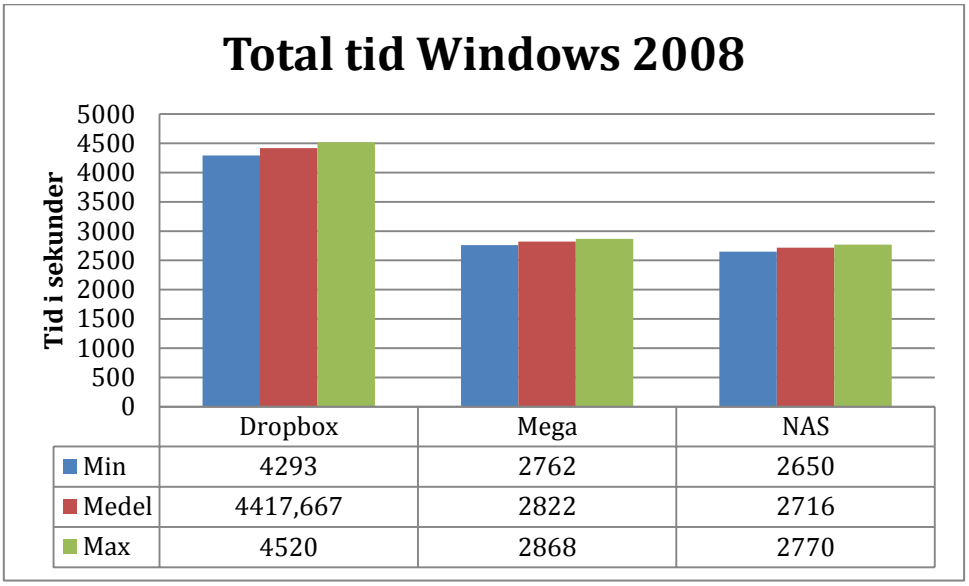


Figur 7.2 – Tid för skapandet av lokal säkerhetskopia samt överförning av denna.

7.2.2 Total tid

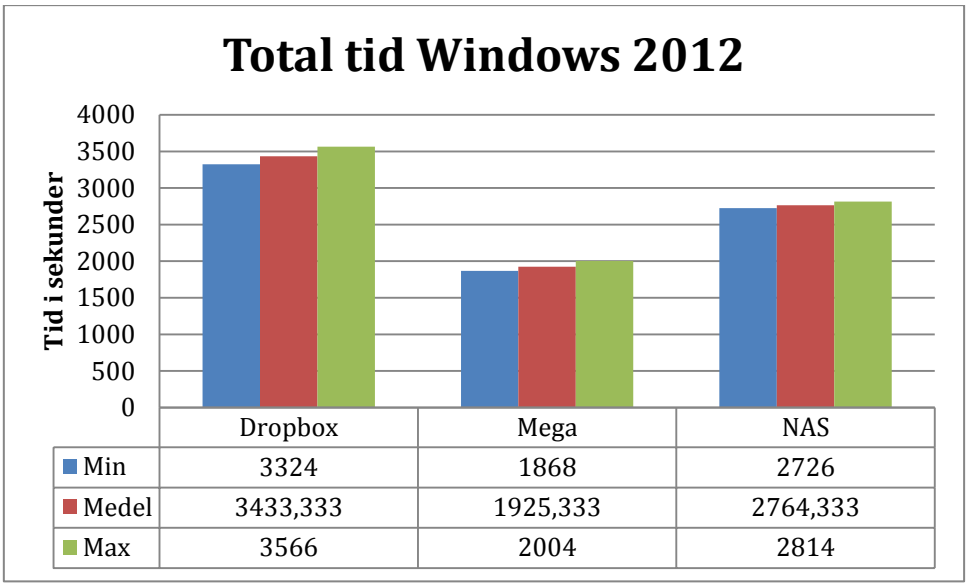
Graf 7.3 och 7.4 redovisar den totala tiden från det att en lokal process för att skapa en säkerhetskopia startas till det att denna säkerhetskopia finns lagrad på molnplattformen. Detta inkluderar den tid det tar att skapa säkerhetskopian lokalt på systemet, eventuell väntatid samt den tid det tar att föra över säkerhetskopian till molnplattformen.

Windows Server 2008 R2



Figur 7.3 - Tid för skapandet av lokal säkerhetskopia, överförning samt väntetid.

Windows Server 2012 R2

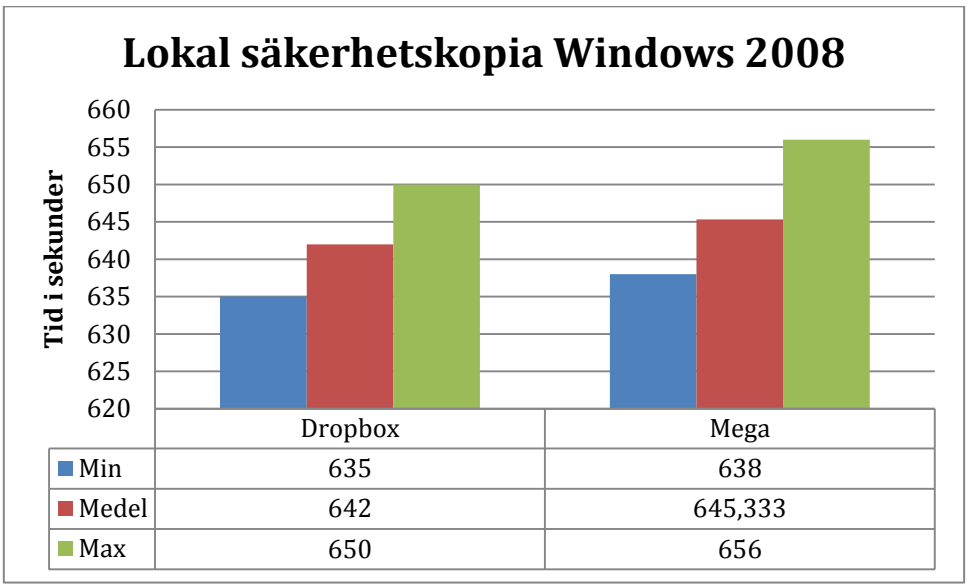


Figur 7.4 - Tid för skapandet av lokal säkerhetskopia, överförning samt väntetid.

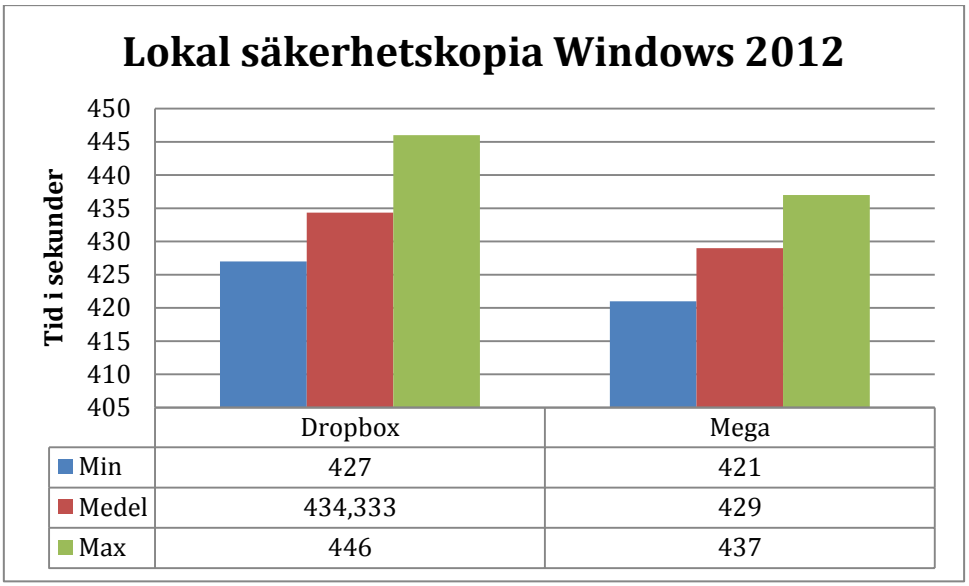
7.2.3 Tid för skapandet av lokal säkerhetskopia

Graf 7.5 och 7.6 presenteras för att kunna särskilja hur lång tid det tar att skapa en säkerhetskopia lokalt på systemet. Detta är dock ingen teknik som fjärrbaserad lagring (NAS) använder sig av, utan denna metod lagrar data direkt på fjärrdatorn varav den inte tas med i detta test.

Windows Server 2008 R2



Figur 7.5 - Tid för skapandet av lokal säkerhetskopia.

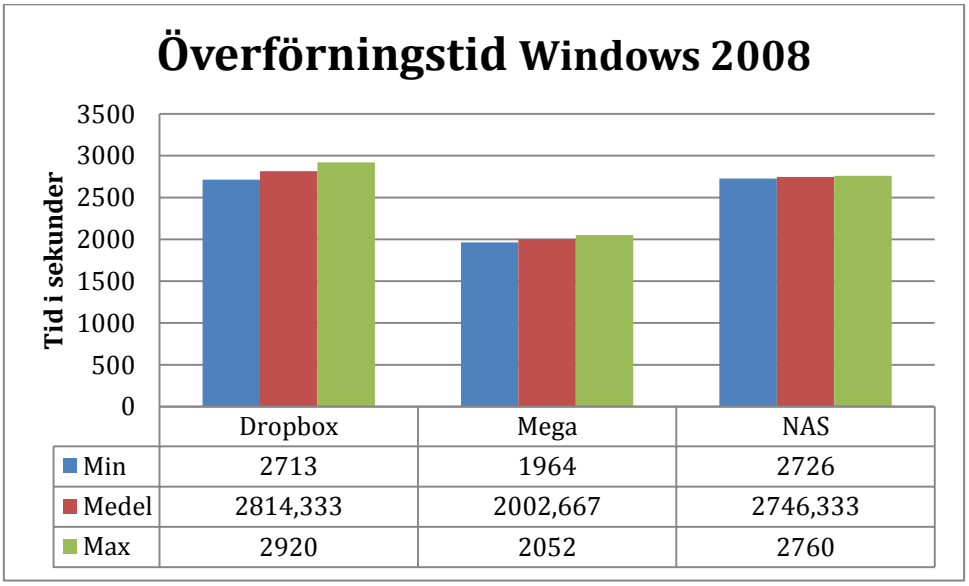


Figur 7.6 - Tid för skapandet av lokal säkerhetskopia.

7.2.4 Tid för att föra över en säkerhetskopia

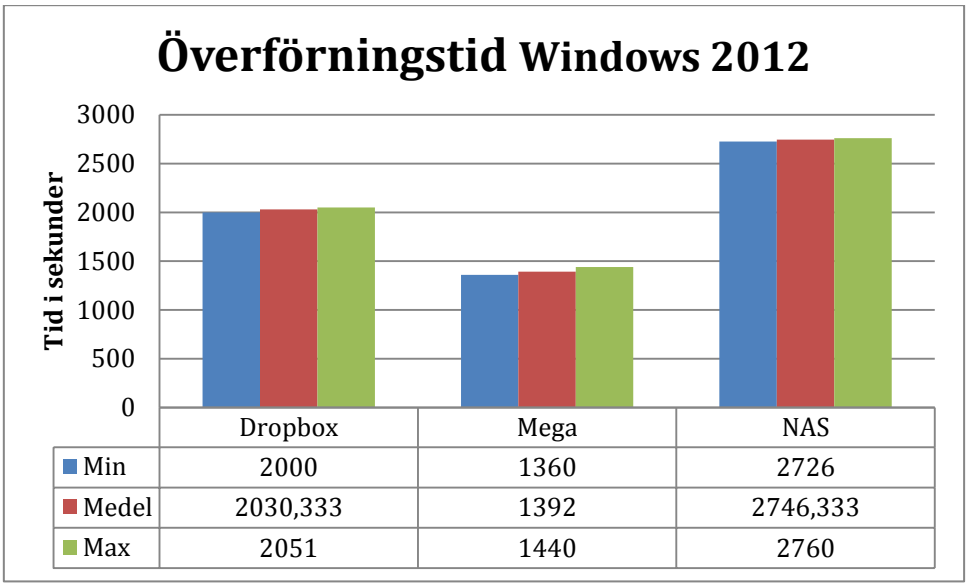
Graf 7.7 och 7.8 presenterar överföringstiden, vilket är den tid som det tar från det att säkerhetskopian är skapad till att denna finns lagrad på molnplattformen. Eventuell mellantid (väntetid eller liknande) är borträknad. D.v.s. enbart den tid det tar att föra över säkerhetskopian till molnplattformen presenteras.

Windows Server 2008 R2



Figur 7.7 - Tid för överföring av säkerhetskopian.

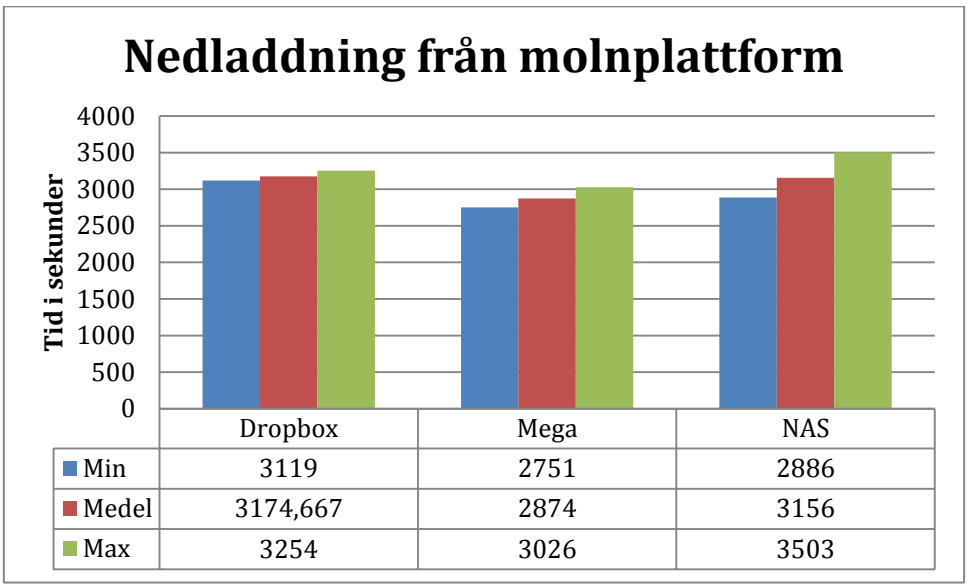
Windows Server 2012 R2



Figur 7.8 – Tid för överförning av säkerhetskopian.

7.2.5 Tid för att ladda ner en säkerhetskopia

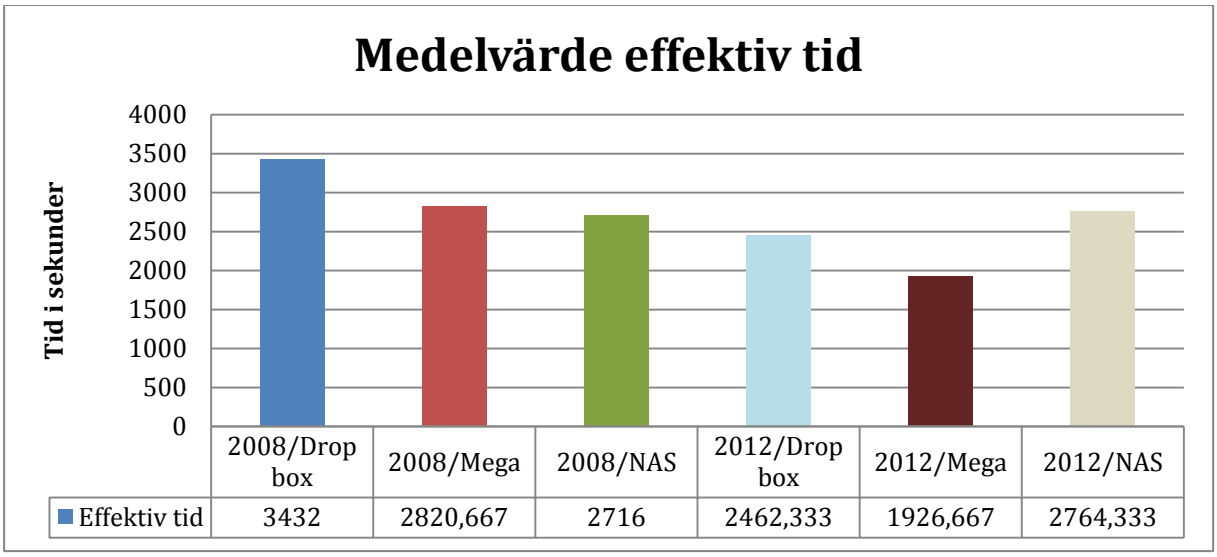
Graf 7.9 presenterar den tid det tar att ladda ner en säkerhetskopia till en dator. Här presenteras enbart nedladdningstiden direkt från molnplattformen och inte själva återställningstiden. Nedladdningen har skett till en server (Windows 2012 R2) som har samma prestanda som tidigare nämnts i sektion 6.2.1.



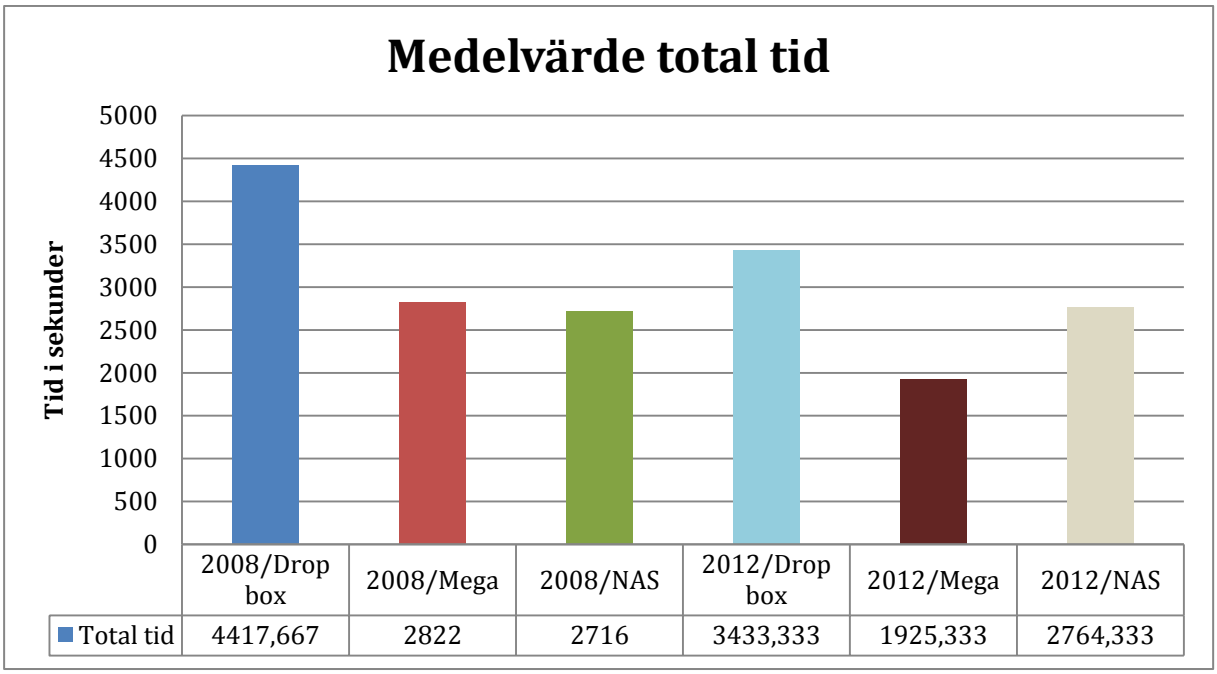
Figur 7.9 – Nedladdning av säkerhetskopia.

7.2.6 Jämförelse molnplattform och operativsystem

Graf 7.10 och 7.11 presenterar medelvärdet av samtliga testkörningar (totalt 3) för varje molntjänst och operativsystem. Graf 7.10 presenterar effektiv tid vilket inkluderar, den tid det tog att skapa en säkerhetskopia lokalt på datorn samt hur lång överförningstid dessa hade. Graf 7.11 presenterar total tid vilket inkluderar den totala tiden från det att en lokal process för att skapa en säkerhetskopia startas till det att denna säkerhetskopia finns lagrad på molnplattformen.



Figur 7.10 – Jämförelse effektiv tid mellan molnplattform och operativsystem.



Figur 7.11 – Jämförelse total tid mellan molnplattform och operativsystem.

7.2.7 Automation och integration

För att skapa en säkerhetskopia lokalt finns möjlighet att schemalägga detta i det inbyggda verktyget ”Schemaläggning av backup” vilket gör det möjligt att skapa en säkerhetskopia utan att en systemadministratör själv sitter och startar processen. På detta vis kommer processen betraktas som automatisk då en systemadministratör inte behöver göra om varje process manuellt varje gång utan istället körs detta efter ett schema som systemadministratören själv bestämmer, baseras på tid och dygn. Med hjälp av detta verktyg finns också möjlighet att spara säkerhetskopian på en extern dator vilket löser hur säkerhetskopian skall lagras på NAS.

När en säkerhetskopia väl är skapad på det lokala systemet lagras denna i en mapp som antingen Mega eller Dropbox synkroniserar. Detta gäller hela mappen och dess undermappar vilket gör det möjligt att alltid lagra den senaste säkerhetskopian på molnplattformen. Både Megas och Dropbox synkroniseringsverktyg installeras på systemet, en användare loggar sedan in på sitt konto och väljer vilka mappar som skall synkroniseras till molnplattformen. En systemadministratör behöver sedan inte lägga större vikt på att konfigurera dessa verktyg då de själva söker efter uppdateringar i synkroniserade mappar och för över ny data till molnplattformen. Varav automation och integrering också går att uppnå här då en användare inte själv behöver ladda upp filer manuellt på molnplattformen för att hålla denna uppdaterad. Synkroniseringsverktygen märker själva av när filer läggs till och uppdateringar görs när nya filer läggs till i mappen, dessa uppdateringsintervaller skiljer en aning men det kan betraktas som automatiskt.

8 Analys

8.1 Litteraturstudie

För att behandla delfråga 1 (*Hur skyddas data när den skickas*), har information som finns publicerat på respektive utgivares hemsida. Dessa två tjänster använder någon sorts av AES kryptering tillsammans med SSL och TLS för att skicka data över Internet. Det råder dock oklarheter om hur stark kryptering som skall användas då t.ex. processorprestanda kan påverkas negativt om för hög kryptering används. Utgivarna av plattformen Mega menar att 128 bitars AES kryptering räcker för att kryptera data då hårdvarubelastningen blir onödigt hög om starkare kryptering används.

Dropbox har en speciell avdelning som sysslar enbart med säkerhetsrelaterade frågor som förespråkar att AES med 256 bitars kryptering bör användas. Detta är också något som kommer att presenteras i experiment om det är någon större skillnad i processorbelastning beroende på om AES-128 eller 256 används.

En annan sak som är intressant är nyckelhanteringen och hur respektive molnleverantör har för åsikter runt dessa. Mega som anser att nyckelhanteringen bör ligga i användarens händer då datan enbart kan läsas av den person som laddar upp datan (med undantag för metadata) medans Dropbox förespråkar att nyckelhanteringen skall ligga hos dem för att underlätta synkronisering av flera enheter till ett konto. Dock erbjuder användaren att själv ha ansvar för nyckelhanteringen.

8.2 Experiment

För att besvara delfråga 2 (*Hur skiljer sig hastigheten och tiden för att skapa en säkerhetskopia samt att göra en återställning från denna beroende på om en molnbaserad plattform eller en traditionell fjärrbaserad lagring används?*) har experiment utförts genom att först skapa en säkerhetskopia lokalt på datorn med “Windows Server backup”. För att lagra denna säkerhetskopia på molnplattformen har synkroniseringsverktyg som finns att ladda ner på respektive molntjänst hemsida använts. Genom att analysera resultaten som har kunnat samlas ihop genom att använda prestandaövervakaren som finns inbyggt i Windows har prestanda för respektive molnplattform kunnat presenteras.

Tidigare i denna studie har tid delats upp i två parametrar, tid för att skapa en säkerhetskopia lokalt och tid för att föra över denna till molnplattformen. I det första experimentet visas den totala effektiva tiden för att skapa en säkerhetskopia till det att den finns placerad på molnplattformen. Detta för att få en överblick om hur respektive teknik fungerar rent praktiskt utan väntetider och liknande. Det andra testet mäter den totala tiden från det att processen startas till det att säkerhetskopian finns tillgänglig på plattformen, detta inkluderar väntetider och liknande, detta för att kontrollera om flaskhalsar kan ligga i synkroniseringsverktyget eller om det är marginell skillnad i prestandabelastning och nätverksbelastning som gör att det blir olika resultat.

Genom att analysera resultaten kan en slutsats dras att av molnplattformarna är Mega snabbast på att transportera en säkerhetskopia från det att en säkerhetskopia skapas lokalt till det att denna ligger på molnplattformen. Det finns också skillnader i vilket operativsystem som används då Windows 2008 R2 använder mindre systemresurser vid dessa aktiviteter än vad Windows 2012 R2 gjorde vilket kan vara en påverkan på resultatet. Dock kan slutsatsen dras att oberoende vilket operativsystem som används prestarer generellt Mega bättre än vad Dropbox gör, speciellt de totala tiderna inklusive väntetider. Då processen övervakades manuellt vid alla tester gjordes observationer att Dropbox synkroniseringsverktyg indexerar filer innan dessa laddas upp på plattformen. Detta skapar långa väntetider vid stora filer (ca 15 minuter). Mega tillskillnad från Dropbox sökte igenom synkroniseringsmappar utan att indexera och startade uppladdningen direkt när nya filer skapades i synkroniseringsmappen.

Hur dessa två tjänster skiljer sig mot en NAS är tydligt från dessa experiment. Mega presterar generellt bättre än vad en traditionell NAS med "Windows server backup". Dock presterade Mega och NAS betydligt bättre än vad Dropbox gjorde, vilket troligtvis beror på den långa indexeringstekniken som används av Dropbox.

Ett sista experiment har gjorts för att behandla delfråga 3 (*Hur schemaläggs aktiviteten i systemet och hur diskret är denna för användare och system administratör?*). Detta för att kontrollera hur integreringen fungerar med operativsystemet samt om automation kan ske fullt ut eller delvis. I detta experiment presenteras inga mätresultat utan en beskrivande text kommer istället att användas.

Transparens. Genom att använda synkroniseringsverktyg som både Mega och Dropbox erbjuder, kan en användare synkronisera filer som ligger lokalt på datorn med molnplattformen. De två olika tjänsterna har liknande upplägg då användaren installerar ett mjukvaruprogram på sitt system, detta program går sedan att nå i verktygsfältet på datorn och är näst intill obemärkt för användaren. Användaren väljer sedan vilka mappar som skall synkroniseras med molnplattformen och beroende på vilka data som finns i dessa mappar kommer dessa data sparas på molnplattformen. På detta sätt kan en säkerhetskopia skapas genom "Windows Server backup" och lagras i en mapp på systemet. Genom att ange att den mappen som säkerhetskopian finns lagrad i skall synkroniseras med molnplattformen kommer säkerhetskopian finnas lagrad på molnplattformen.

Tjänsten Mega har visats sig ha korta uppdateringsintervaller, d.v.s. synkroniseringsverktyget märker snabbare av ändringar i mappar genom att t.ex. nya filer läggs till eller tas bort. Detta kommer att påverka slutresultat för den totala tiden från det att en säkerhetskopia skapas till det att denna finns på molnplattformen. Detta då Dropbox använder sig av indexering och ladda ner filstrukturer till den lokala datorn med långa uppdateringsintervaller, detta leder till att den totala tiden blir längre då inte ändringar märks direkt när dessa görs.

Automation. Då synkroniseringsverktyget aktivt söker efter nya uppdateringar i de mappar är aktiva att synkronisera läggs ny data till allt eftersom på molnplattformen beroende på vad som lagras på den lokala datorn. Då "Windows server backup" har använts som verktyg för att skapa säkerhetskopior är det fullt möjligt att använda den inbyggda schemaläggaren för att automatisera processen vilket leder till att en systemadministratör inte själv behöver sitta och starta denna process. Då synkroniseringsverktyget hela tiden söker efter uppdateringar kommer också säkerhetskopior att lagras på molnplattformen.

Med denna teknik kan hela processen betraktas som automatisk då en systemadministratör enbart behöver lägga fokus på att utveckla en schemaläggningsplan och se till så att säkerhetskopian har en synkroniseringsmapp som målmapp för denna säkerhetskopia.

Då bägge molntjänster använder sig av likande teknik rent hur filer sparas lokalt för att sedan synkroniseras med molnplattformen är bägge automatiska då en användare enbart behöver ange vilka mappar som skall synkroniseras, programmet sköter sedan resten. Det är alltså ingen större skillnad från ett automatiskt perspektiv.

Återställning. Dessa resultat är någorlunda likvärdiga i två av tre test presterar Dropbox sämst när en säkerhetskopia skall laddas ner. Detta kan bero på att som tidigare nämnts hanterar Dropbox all nyckelhantering internt vilket kan påverka då dekrypteringen måste ske mot en av Dropbox servrar vilket kan skapa extra sessioner och fler kontroller måste göras. Dock skiljer inte dessa resultat något anmärkesvärt vilket en slutsats kan dras att oberoende tjänst en användare använder sig av behövs inte detta prioriteras högt vid val av molntjänst alternativt NAS.

9 Slutsats

Detta kapitel sammanfattar och avslutar denna studie genom att besvara frågeställningen som användes samt de resultat som presenteras i denna studie. En diskussion presenteras där studien tas ur sitt sammanhang och diskuteras mer öppet. Framtida studier presenteras också för att ge hypotetiska förslag om hur studien skall kunna vidareutvecklas i framtiden.

9.1 Sammanfattning

Denna studie har granskat och analyserat prestanda, integration och säkerhet hos Dropbox och Mega, för att sedan jämföra dessa med en NAS (Network attached storage). Två operativsystem har använts i denna studie, Windows server 2008 R2 och Windows server 2012 R2. Storlek på säkerhetskopian har varit konstant i samtliga experiment (13,9 GB), vilket speglar en säkerhetskopia av Windows server 2012 R2 med vanligt förekommande tjänster (DNS, DHCP, Active Directory, Windows server backup samt ett antal delade mappar med innehåll).

De experiment som utfördes i denna studie testade tjänsternas: Totala effektiva tid (exklusive eventuella väntetider), totala tid (inklusive väntetider), skapande av lokal säkerhetskopia, tid för överförning av säkerhetskopia samt tid för nedladdning från molnplattform. Även en analys av litteraturstudie genomfördes med inriktning på säkerhet och integritet.

För att besvara den övergripande frågan ”Hur skiljer sig lagring av säkerhetskopior på en molnbaserad plattform mot en NAS (Network attached storage) med avseende på prestanda, integration och integritet”, delades denna in i tre delfrågor.

Delfråga 1, ”Hur data skyddas när den skickas”, besvarades genom en litteraturanalys. Denna visar att Dropbox har starkare säkerhet än vad Mega har. Dropbox prioriterar säkerhet och använder AES-256 bitars kryptering för att föra över data, Mega använder AES-128 bitars kryptering. Den ökade säkerhet som Dropbox erbjuder genom starkare kryptering medför prestandaförluster. Skillnader finns också i hur de olika tjänsterna hanterar krypteringsnycklar, Dropbox ansvarar själva för all nyckelhantering. Mega låter istället respektive användare hantera sina egna krypteringsnycklar.

Delfråga 2, ”Hur hastigheten och tiden varierar för att skapa en säkerhetskopia samt göra en återställning från denna beroende på om en molnbaserad plattform eller en traditionell fjärrbaserad lagring används”, besvarades genom att utföra experiment. Utfallet av experiment gällande uppladdning till molnplattform påvisade att Mega generellt presterar bättre än vad Dropbox gör i samtliga test. Experiment gällande effektiv tid påvisar att skillnaderna mellan alla tre tjänster (Dropbox, Mega och NAS), inte skiljer lika mycket som experiment gällande total tid gör. Total tid inkluderar väntetider, vilket påverkar resultatet, Dropbox använder indexering av filer innan en överförning kan startas vilket resulterar i att den totala tiden blir betydligt längre än vad den blir för Mega och NAS.

Tjänst och operativsystem som presterade bäst gällande effektiv tid med hänsyn till medelvärde, resulterade i att Mega installerad på Windows server 2012 R2 presterade bäst (1926,667 sekunder). Sämst presterade Dropbox installerad på Windows server 2008 R2 (3432 sekunder). Detta påvisar att resultat av molntjänster även påverkas av vilket operativsystem som används. Anledning till att Dropbox presterar sämre än Mega nämndes i analysen, att Dropbox använder en starkare kryptering än vad Mega använder.

Tjänst och operativsystem som presterade bäst gällande total tid med hänsyn till medelvärde, påvisar att Mega installerad på Windows server 2012 R2 presterar bäst (1925,333 sekunder), Dropbox presterar sämst oberoende operativsystem (2008 R2 – 4417,667 sekunder och 2012 R2 - 3433,333 sekunder), Anledningen till detta nämndes i analysen då Dropbox indexerar filer innan dessa förs över till molnplattformen.

Experiment gällande nedladdning från molnplattform presenterar hur lång tid det tar att ladda ner en säkerhetskopia till en dator, detta experiment påvisade att Mega presterar bäst med ett medelvärde på 2874 sekunder, NAS ett medelvärde på 3156 sekunder och Dropbox 3174,667 sekunder.

Delfråga 3, ”Hur aktiviteten schemaläggs i systemet och hur diskret denna är för användare och systemadministratör”, besvarades genom att presentera hur processen går till för att skapa en säkerhetskopia från det att denna startas till denna finns lagrad på molnplattformen, samt eventuella tillägg och extratjänster som erbjuds. Både Mega och Dropbox använder sig av mappar som synkroniseras med molnplattformen. Denna mapp kontrolleras mot existerande filer som finns lagrade på molnplattformar för att synkronisera nya filer som läggs till eller tas bort. När nya filer sparas i synkroniseringsmappen överförs dessa automatiskt till molnplattformen.

Utefter sammanfattande resultat kan slutsatsen dras att när säkerhet värderas högt och ett krav när en molnplattform skall väljas, så är Dropbox att rekommendera. Är prestanda ett krav, dvs säkerhetskopior skall gå snabbt att skapa och lagra är Mega att rekommendera, då denna tjänst presterar generellt bättre. Båda tjänsterna använder ungefär samma teknik för att föra över säkerhetskopior till molnplattformen, genom synkroniseringsmappar. Jämförelse mellan molnplattformar och en NAS påvisar resultaten att NAS presterar generellt bättre än vad Dropbox gör, men inte bättre än Mega. Integration när en NAS används för över säkerhetskopian samtidigt som denna skapas i Windows server backup, dvs ingen synkroniseringsmapp används. Båda molntjänsterna använder någon typ av kryptering.

9.2 Diskussion

Denna studie behandlar två stycken molntjänster, Dropbox och Mega, som är installerade på två olika operativsystem (Windows server 2008 R2 och Windows server 2012 R2). Detta för att ge läsaren en överblick över hur dessa molntjänster presterar mot varandra men också för att jämföras med en traditionell lagringsmetod som erbjuds via NAS. Denna studie ger en överblick över prestanda, säkerhet samt integration.

För att testa prestanda har enbart denna studie behandlat en konstant storlek av en säkerhetskopia (13,9 GB). Ett alternativ kan också vara att testa hur prestanda skiljer sig mellan flera olika filstorlekar. Detta är dock inget denna studie behandlar, istället finns detta nämnt som förslag i kapitel 9.3 Framtida studier. För att bestämma storleken på säkerhetskopian har författaren av denna rapport och handledare arbetat fram ett exempel som speglar hur en server med tillhörande tjänster kan vara utformad i en industriell miljö. Vilket resulterade i tjänster som t.ex. DHCP, DNS, Active Directory, Windows server backup samt ett antal delade mappar med innehåll. Detta för att adressera den externa validiteten som beskrivs i kapitel 4,2 med hänsyn till förmågan att generalisera resultat av experiment i en industriell tillämpning.

För att testa prestanda var det planerat att även inkludera andra resursbelastningar som t.ex. CPU-belastning, RAM-användning och belastning på hårddisk. Dock var dessa data svårare att samla in, presentera på ett lämpligt sätt samt sammanfatta. Författaren av denna rapport och handledare kom istället fram till att fokus skulle ligga på åtkomsttid för respektive molnplattform, då tiden inte räckte till. Därför förkastades idén om att även inkludera andra resursbelastningar och nämns istället som förslag i kapitel 9.3 Framtida studier.

Alla tekniker som används i denna studie kan betraktas som automatiska. Schemaläggning är möjlig för dessa aktiviteter, då Windows server backup kan lagra säkerhetskopior direkt i synkroniseringsmappar som både Dropbox och mega använder, dessa synkroniseringsverktyg började inte föra över några filer tills det att alla andra processer var helt avslutade, d.v.s. till dess att säkerhetskopian är klar.
De validitetshot som berör litteraturstudien som finns identifierade i sektion 4.1, har till stor del gått att uppfyllas. Dvs informationen som presenteras i resultatet av litteraturstudien är uppdaterad vid publicering. Informationen som denna studie presenterar är mestadels hämtad från pålitliga källor som tex vetenskapliga databaser och officiell hemsida för respektive molnplattform.

Validitetshot som berör experiment finns identifierade i sektion 4.2, har delvis besvarats i resultaten. Problemet med pålitlighet åtgärdades genom att utföra test ett flertal gånger vid olika tidpunkter för att kontrollera om resultat blev likvärdiga. Detta genom att schemalägga aktiviteter för att skapa säkerhetskopior. Värt att nämnas är att även om schemaläggning användes övervakades varje testkörning manuellt.

Ett annat problem är validitet med hänsyn till konstruktion samt slumpmässig irrelevans i experimentell uppsättning, dessa kunde stärkas genom att innan varje testkörning kontrollera så att aktivitetshanteraren visade 0 % utnyttjande.

9.3 Framtida studier

Framtida studier kan behandla hur en systemåterställning presterar genom att direkt återställa från respektive molnplattform. I denna studie måste en säkerhetskopia först laddas ner till en extern enhet, för att sedan återställas från denna enhet. Det kan också vara intressant att se hur resultat påverkas av att direkt kunna återställa från en molnplattform.

Denna studie använder enbart de synkroinseringsverktyg som respektive utgivare publicerat på de officiella hemsidorna. Möjligheten finns också att ladda upp filer direkt i webbläsaren, vilket en framtida studie kan behandla för att jämföra aspekter som prestanda och om analys av litteraturstudie ger likvärdigt resultat.

P.g.a. tidsbrist så var det inte möjligt att även kontrollera hur kontinuerliga och inkrementella säkerhetskopior presterar på molnplattformar. Detta är ett område som framtida studier kan behandla för att adressera hur dessa tekniker skiljer sig på en molnbaserad lagring av säkerhetskopior.

I denna studie behandlas som tidigare nämnts enbart en konstant filstorlek, framtida studier kan behandla hur dessa molntjänster presterar vid flera olika filstorlekar. Detta för att kontrollera om resultaten är likvärdiga eller om resultaten skiljer sig beroende på filstorlekar. Andra resursbelastningar kan också behandlas i denna del, som t.ex. CPU-belastning, RAM-användning och belastningar på hårddisk.

Referenser

Berndtsson, M., Hansson, J., Olsson, B., och Lundell, B. (2008). *Thesis Projects: A Guide for Students in Computer Science and Information Systems, 2nd ed*, Springer Verlag.

Chang, G., Shams, K., Callas, J., & Kern, A. (2012). A Novel Approach to Automated, Secure, Reliable, & Distributed Backup of MER Tactical Data on Clouds. Paper presented at the Aerospace Conference, 2012 IEEE.

Dropbox (2014a). *Dropbox release notes*. Tillgänglig: https://www.dropbox.com/release_notes [Hämtad: 2014-06-04]

Dropbox (2014b). *Dropbox for Business Security – A Dropbox whitepaper*. Tillgänglig: https://www.dropbox.com/static/business/resources/Security_Whitepaper.pdf [Hämtad: 2014-06-08]

Dropbox (2014c). *How secure is Dropbox?*. Tillgänglig: https://www.dropbox.com/help/27/en [Hämtad: 2014-06-08]

Dropbox (2014d). *Everything you need to work smarter*. Tillgänglig: https://www.dropbox.com/business/pricing [Hämtad: 2014-08-21]

Fisher, T. (2014). *38 Online Backup Services Reviwed*. Tillgänglig på: http://pcsupport.about.com/od/maintenance/tp/online_backup_services.htm [Hämtad: 2014-02-25].

Hanavan, P. (2007) *An Overview of Continous Data Protection*. Tillgänglig: http://www.infosectoday.com/Articles/Continuous_Data_Protection.htm [Hämtad: 2014-06-05]

Johansson, R. (2013). *Hur påverkas säkerhetskopiering av prokrastinering*. (Student paper). Högskolan i Skövde. Tillgänglig: http://urn.kb.se/resolve?urn=urn:nbn:se:his:diva-8248 [Hämtad: 2014-06-06]

Machani, S., M'Raihi, D., Pei, M., & Rydell, J. (2011). *TOTP: Time-Based One-Time Password Algorithm*. Tillgänglig: http://tools.ietf.org/html/rfc6238 [Hämtad 2014-04-29].

Mega (2014a). *Mega limited terms of service ("TERMS").* Tillgänglig: https://mega.co.nz/#terms [Hämtad: 2014-16-07]

Mega (2014b). *Developers – Documentation*. Tillgänglig: https://mega.co.nz/#doc [Hämtad: 2014-06-07]

Mega (2014c). *Help centre – security & privacy*. Tillgänglig: https://mega.co.nz/#help/security [Hämtad: 2014-06-07]

Mega (2014d). *MEGA Sync Client: Easy automated syncing between your computers and your MEGA cloud drive*. Tillgänglig: https://mega.co.nz/#sync [Hämtad: 2014-06-04]

Patel, H., Patel, D., Chaudhari, J., Patel, S., & Prajapati, K. (2012). *Tradeoffs between performance and security of cryptographic primitives used in storage as a service for cloud computing*. Paper presented at the Proceedings of the CUBE International Information Technology Conference, Pune, India, S. 557-560.

Pearson, S. (2009). *Taking account of privacy when designing cloud computing services.* Paper presented at the Software Engineering Challenges of Cloud Computing, 2009. CLOUD '09. ICSE Workshop on. S. 44-52.

Rouse, M. (2010). I*ncremental backup*. Tillgänglig: http://searchdatabackup.techtarget.com/definition/incremental-backup [Hämtad: 2014-06-05]

Sinanc, D., & Sagiroglu, S. (2013). *A review on cloud security*. Paper presented at the Proceedings of the 6th International Conference on Security of Information and Networks, Aksaray, Turkey.

Sundaresan, S., Donato, W. d., Feamster, N., Teixeira, R., Crawford, S., Pescap, A. (2011). *Broadband internet performance: a view from the gateway*. Paper presented at the Proceedings of the ACM SIGCOMM 2011 conference, Toronto, Ontario, Canada.

Techsoup Global. (2012). *2012 Global Cloud Computing Survey Result*. Tillgänglig på: https://www.techsoup.se/sites/default/files/2012_Global_Cloud_Survey_Full_Report.pdf [Hämtad: 2014-02-25].

Traeger, A., Joukov, N., Sipek, J., & Zadok, E. (2006). *Using free web storage for data backup*. Paper presented at the Proceedings of the second ACM workshop on Storage security and survivability, Alexandria, Virginia, USA, S 73-78

Wohlin, C., Runeson, P., Höst, M., Ohlsson, M. C., Regnell, B., & Wesslén, A. (2012). *Experimentation in Software Engineering*. Berlin, Heidelberg: Springer Berlin Heidelberg. ISBN: 978-3-642-29043-5, S.104-112,