1.Introduktion

1.1 Inledning

Den senaste trenden inom IT-världen är cloud computing (molntjänster). Molntjänster har uppnått stor popularitet både hos IT-chefer och ekonomichefer inom stora företag. Molntjänster anses vara en av de 10 viktigaste teknologiska strategierna för företag 2011 [1].

Med molntjänster avses processorkraft, lagringsutrymme och applikationer som finns på servrar i en eller flera datorhallar vilka kunden får åtkomst till via internet. Dessa tjänster säljs i form av applikationer, Software as a Service (SaaS), IT-infrastruktur, Infrastructure as a Service (IaaS) och processorkraft, Platform as a Service (PaaS).

Molntjänsterna debiteras efter användning, vilket medför att de (i teorin) är gratis då de ej används, vilket tilltalar de ekonomiansvariga i företagen [2]. Det kräver inget initialt investeringsbehov och ingen egen spetskompetens för att underhålla IT-miljön.

En ytterligare fördel med molnet är att servrarna används effektivare och bättre nyttjar servrarnas resurser, vanligtvis utnyttjas inte hårdvaran till fullo. Med virtualisering kan flera system köras på samma server. Då nyttjas hårdvarukapaciteten till en högre grad vilket medför att färre antal fysiska servrar behövs. Detta är bra för miljön då det minskar materialåtgång och energiförbrukning. När en server närmar sig sin maxkapacitet ger virtualisering en möjlighet att migrera gästsystem till en annan server.

Under 60 och 70 -talet var virtualisering ett hett område inom datalogin då hårdvaran ofta var dyr och krävde stor plats. Att då kunna köra flera maskiner på samma hårdvara var en stor fördel. En ytterliggare fördel med virtuellt minne var att applikationerna nu kunde presenteras med ett näst intill oändligt kontinuerligt minne. Detta medförde att programmeraren inte behövde ladda in olika programdelar i minnet, istället fick hela programmet plats i minnet [25]. I takt med att kostnaden för hårdvaran sjönk minskade intresset för virtualisering. Nu med bland annat molnet har virtualisering återigen fått ett uppsving vilket medfört att hårdvaruleverantörer har konstruerat stöd för virtualisering i sina nya produkter.

1.2 Bakgrund

Det som idag gör företag osäkra till att investera i molntjänster är säkerhetsaspekterna [4]. De allra flesta företag hanterar information som är känslig och de har krav på hur sådan information får hanteras. Denna typ av information kan exempelvis vara personal- eller kundinformation. Molntjänster gör att det finns många säkerhetsaspekter att ta hänsyn till då mycket information finns lagrad på samma plats. Det som oroar företagen är de risker som existerar då informationen skickas över internet, hur information lagras hos molnleverantören, hur molnleverantörerna hanterar den lagrade informationen samt att flera företag exekverar flera Virtuella Maskiner (VM) på samma server. En hypervisors uppgift är att isolera VM från varandra för att säkerställa att information ej hamnar i fel händer.

Hårdvarustödet för virtualisering har utvecklats på senare år med bland annat AMD-V. Detta medför att hypervisorn blir mindre komplex eftersom den kan dra nytta av hårdvaran [17]. Det finns vissa skillnader i hur man bygger en hypervisor och dessa skillnader är beroende av vilken arkitektur som ska virtualiseras.

Enligt Popek och Goldberg [32] existerar tre krav som bör uppfyllas av en hypervisor.

1. Exakthet, mjukvara som körs i en VM ska exekvera exakt som det gör när det exekverar direkt på hårdvaran.
2. Prestanda, En stor mängd av mjukvarans instruktioner ska kunna utföras utan hypervisorns inblandning.
3. Säkerhet, hypervisorn ska kontrollera all hårdvaruåtkomst.

Man kan alltså sammanfatta detta till att hypervisorn ska vara transparent så att mjukvaran i en VM inte uppfattar att den virtualiseras. Hypervisorn ska dessutom säkerställa isolering och korrekthet så att en VM endast kan komma åt sin egen information, vilket medför säkerhet.

1.3 Syfte

Molntjänster bygger på virtualisering. Virtualiseringslagret ska delge hårdvaruresurser till de molntjänster som exekverar på en server hos en molnleverantör. Dessutom ska virtualiseringen skapa isolering mellan molntjänsterna. För företag är denna isolering oerhört viktig och ett orosmoln för IT-ansvariga hos de företag som planerar att införskaffa

molntjänster. För att isolering ska fungera korrekt krävs att minnet hos de virtuella maskinerna är korrekt isolerade från varandra.

Syftet med uppsatsen är att studera hur minne virtualiseras hos några av de hypervisors som används i dagens molntjänster. Fokus ligger på minnesisolering, då denna är en central del i informationssäkerheten för molntjänsten. Ytterligare en central aspekt är hypervisorns prestanda som påverkas av hårdvarustödet hos den hårdvara som virtualiseras.
För att söka svar på syftet har vi undersökt minnesvirtualisering i två hypervisors Xen och VMWare. Vi har dessutom undersökt det hårdvarustöd för virtualisering som lanserats av hårdvarutillverkarna AMD och Intel.

1.5 State of The Art

En hypervisors uppgift är att virtualisera de resurser hårdvaran erbjuder i form av Central Processing Unit (CPU), minne och I/O samt att skapa en virtualiserad miljö. Denna miljö är mer känd som en VM. Fler VM:s kan köra på samma maskin och får åtkomst till hårdvaran via hypervisorn. Vi kommer här redogöra för några olika State-of-The-Art hypervisors som används i dagsläget.

1.5.1 Xen Hypervisor

Xen Hypervisor används bland annat i molntjänsten Amazon Web Services. Xen körs på x86 processorarkitekturen och denna arkitektur är tämligen svår att virtualisera då den inte har hårdvarustöd för att virtualisera CPU, minne och I/O [9, 10, 11]. Detta medför att hypervisorn blir betydligt mer komplex i förhållande till om hårdvarustöd för virtualisering existerat. Enligt Xen själva är deras prestanda nära inpå den prestanda som hårdvaran kan prestera om den körs utan Xen Hypervisor [11].

1.5.2 VMWare ESXi

ESXi använder sig av privilegierade ringar i fyra nivåer, från ring 0 som är den lägsta men mest privilegierade ringen till ring 3 med minst privilegier. I ring 0 körs hypervisorn, VM körs i ring 1 medan applikationer i VMs exekveras i ring 3. Varje VM innehåller ett komplett system med exempelvis CPU och BIOS. Vilket OS som helst kan användas i ESXi, till skillnad från de övriga hypervisors vi undersökt [18].

1.5.3 Microsoft Hyper-V

Hyper-V exekveras på en utveckling av den arkitektur som Xen exekveras på x86-64 processorarkitektur, vilken har stöd för virtualisering i hårdvaran [1]. Hyper-V används tillsammans med Windows Server 2008 eller en Server Core. Isolering sker genom partitioner där OS exekveras [13]. Windows Server Hyper-V inkluderar syntetiska drivrutiner, vilket resulterar i prestandaförbättring då detta reducerar antalet gånger CPU:n behöver byta mellan kernel-mode och user-mode [13].

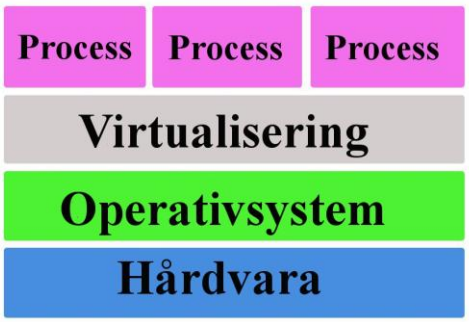
2. Virtualisering

Virtualisering är en abstraktion av ett datorsystem, där ett lager av virtualiseringslogik tillhandahåller och hanterar virtualiserade resurser till en klient [9]. Goldberg liknar en VM vid en avbild av ett eller flera kompletta system [7]. Enligt Mallach ger även Goldberg definitionen av virtualisering som:
”*A system … which … is a hardware-software duplicate of a real existing machine, in which a non-trivial subset of the virtual machine's instructions execute directly on the host machine...”* [8].
Som följd av dessa definitioner kan man säga att virtualisering handlar om att ge en eller flera VM en illusion av att de har ensam tillgång till hårdvarans resurser.

Enligt Douglas och Gehrmann är de två mest framträdande virtualiseringsformerna processvirtualisering och systemvirtualisering [9]. En likartad uppfattning har Daniels som menar att det finns 3 typer av virtualisering: mjukvaruvirtualisering, hårdvaruvirtualisering och containers [6]. Ur beskrivningen av dessa typer av virtualiseringar kan man dra slutsatsen att mjukvaruvirtualisering och processvirtualisering är samma typ av virtualisering. På samma sätt är hårdvaruvirtualisering och systemvirtualisering även dessa samma typ av virtualisering. Det som skiljer Douglas och Gehrmanns syn på virtualisering med Daniels är således containers. Vid systemvirtualisering virtualiseras hårdvaran till ett gästande operativsystem till skillnad mot processvirtualisering där hårdvaran virtualiseras till en applikation som exekveras i ett operativsystem. Systemvirtualisering kan uppnås med hjälp av paravirtualisation, containers eller ISA-översättning. I detta kapitel studeras och beskrivs olika typer av virtualisering. Detta kommer sedan att leda in på hypervisors vilket studeras i efterföljande kapitel.

2.1 Processvirtualisering

Vid processvirtualisering ligger virtualiseringslagret mellan OS och VM [6]. OS virtualiserar systemets resurser såsom minne, CPU och andra enheter. Vilket leder till att varje exekverande process erhåller intuitionen av full tillgång till hårdvarans resurser [9]. Av dessa definitioner kan vi dra slutsatsen att processvirtualisering sker mellan OS och de processer som exekveras, vilket visas i figur 1. Det krävs alltså att de processer som exekveras är designade för det OS som de exekverar i. Enligt Douglas och Gehrmann är processvirtualisering ett fundamentalt koncept i varje modernt operativ system. I dagens datorer exekverar flera processer samtidigt, processvirtualiseringen isolerar dessa processer från varandra och erbjuder processen en illusion av full åtkomst till hårdvaran.



Figur 1, Processvirtualisering

2.2 Systemvirtualisering

Vid systemvirtualisering virtualiseras hela datorsystemets miljö. Virtualiseringslagret mellan hårdvaran och VM benämns hypervisor eller Virtual Machine Monitor(VMM). Hypervisorn är en mjukvara som exekveras på hårdvaran för att virtualisera hårdvaran för VM. Hypervisorn har således till uppgift att hantera och fördela hårdvarans resurser mellan VM [9], vilket illustreras i figur 2. I uppsatsen studeras denna typ av virtualisering och hur dessa hypervisors virtualiserar minne till VM. Då det är denna virtualisering som används av molntjänstleverantörerna idag [10].