KANDIDATEXAMENSARBETE INOM KOMMUNIKATIONSSYSTEM, GRUNDNIVÅ, 15 HP
STOCKHOLM, SVERIGE 2015

Moln för Försvarsmakten

SAJAVAL CHOUDREY & KIM HILTUNEN

KTH KUNGLIGA TEKNISKA HÖGSKOLAN
INFORMATIONS- OCH KOMMUNIKATIONSTEKNOLOGI

Moln för Försvarsmakten

Sajaval Choudrey och Kim Hiltunen

2015-08-14

Kandidatexamensarbete för civilingenjörsexamen
Kursnummer IK121X

Examinator och akademisk handledare
Gerald Q. Maguire Jr.

Extern handledare hos Försvarsmakten
Ross Tsaglidis

KTH Kungliga Tekniska Högskolan
Skolan för Informations- och kommunikationsteknik (ICT)
SE-164 40 Kista/Stockholm, Sverige

Sammanfattning

En organisation med ett så stort ansvar som Försvarsmakten behöver ständigt nya sätt att utvecklas och effektivisera sin drift, administration och organisation. Ett informationshanteringssystem i molnmiljö som grund skulle innebära en modernisering av administrationen inom organisationen och har potentialen att uppfylla Försvarsmaktens förbättringskrav. Arbetet har som huvudmål att ta fram och analysera lösningsförslag för hur Försvarsmakten skulle kunna använda sig av molnbaserade IT-system. I den första delen av arbetet ges en grundläggande introduktion till molnteknologin som även innefattar säkerhetsaspekter. Efter detta presenteras allmän information om Försvarsmakten, deras nuvarande IT-system samt de krav som ställs när det kommer till implementation av nya IT-system inom organisationen. Två olika molntjänster från WMware och Cloudstack undersöks för att se hur dessa skulle kunna användas för en eventuell implementation inom Försvarsmakten. Analysen av de två olika molntjänsterna fokuserar främst på säkerhetsaspekter, då det är ett viktigt fokusområde för Försvarsmakten.

Ett annat område som arbetet har som syfte att undersöka är ekonomin för molntjänster. Detta för att se om en eventuell implementation är lönsam för Försvarsmakten eller inte.

Nyckelord

Moln, Försvarsmakten, datasäkerhet, molnbaserat IT-system

Abstract

An organization with such a big responsibility as the Swedish armed forces constantly needs to find new ways to develop and increase their effectiveness when it comes to management, administration and organization. An information system with cloud computing as a basis would mean a modernization of the Swedish armed force's administration and could potentially live up to the security standards within the organization. The primary goal of the thesis is to present and analyze cloud solutions that the Swedish armed forces eventually could integrate in to their activities. The first part of the thesis gives an introduction to the cloud technology with the security aspects of a cloud as a large part of the focus. This is followed by information about the Swedish armed forces and their current IT-systems, as well as information on the requirements they have for the implementation of new IT-systems within the organization. Two different cloud services from VMware and Cloudstack have been examined in order to see whether these could be used for a future implementation. The focus of the analysis lies heavily on the security issues and questions, that arise, for each solution, as the security aspect is something that is very important for the Swedish armed forces.

The thesis also touches on the economical benefits and economical difficulties associated with cloud service implementation. The purpose of this is to see whether an eventual implementation is beneficial or not.

Keywords

Cloud, Swedish Armed Forces, data security, cloud based IT system

Förord

Vi skulle först och främst vilja tacka Gerald Q. Maguire Jr. för hans vägledning, engagemang i arbetet och ständiga hjälpsamhet.

Tack Ross Tsaglidis, handledare från Försvarsmakten, för att vi fick möjligheten att skriva detta arbete och för all den hjälp du gett oss under arbetets gång.

Vi vill också tacka Openstack Foundation för att vi under detta arbete fick tillgång till att använda oss av bilder från hemsidan.

Stockholm, August 2015
Sajaval Choudrey & Kim Hiltunen

Innehållsförteckning

Sammanfattning i
Nyckelord i
Abstract iii
Keywords iii
Förord v
Innehållsförteckning vii
Lista på figurer ix
Lista på tabeller xi
Lista på akronymer och förkortningar xiii
1 Introduktion 1
1.1 Bakgrund 1
1.2 Problemdefinition 1
1.3 Syfte 1
1.4 Mål 2
1.5 Undersökningsmetod 2
1.6 Avgränsningar 2
1.7 Rapportens disposition 2
2 Bakgrund 5
2.1 Vad är molnet? 5
2.1.1 Typer av moln 5
2.1.2 Servicemodeller för moln 6
2.2 Säkerhet 7
2.2.1 Säkerhet i molnet 7
2.3 Försvarsmakten 8
2.3.1 Försvarsmaktens nuvarande system 8
2.3.2 Implementation av nya IT-system i Försvarsmakten 8
2.3.3 Säkerhetsfunktioner 9
2.3.4 Skyddsaspekter 9
2.4 Informationssäkerhetsklasser hos Försvarsmakten 10
2.4.1 Hemlig/Top secret 10
2.4.2 Hemlig/Secret 10
2.4.3 Hemlig/Confidential 10
2.4.4 Hemlig/Restricted 10
2.4.5 Ej sekretess 11
2.5 Relaterade arbeten 11
2.5.1 Nystartad design av elastiska, anpassningsbara och säkra värdar (CRASH) 11
2.5.2 Uppdragsorienterade elastiska moln (MRC) 11
2.5.3 Säkerhet för molnbaserade tjänster 11
2.5.4 Molnet – möjligheter och begränsningar 11

2.6 Sammanfattning av bakgrund 12
3 Metod 13
3.1 Forskningsprocess 13
3.1.1 Steg 1: Definiera problemet 13
3.1.2 Steg 2: Insamling av lämplig information 13
3.1.3 Steg 3: Framtagning av lösningsförslag 14
3.1.4 Steg 4: Analys och val av lösningsförslag 14
3.2 Insamling av information 14
4 En eventuell implementation hos Försvarsmakten 15
4.1 Publikt moln hos Försvarsmakten 15
4.1.1 Användningen av tredje part 15
4.1.2 Kryptering 15
4.1.3 Nyckel-hashade funktioner 15
4.1.4 Vaktposter 16
4.2 Privat moln hos Försvarsmakten 16
4.3 Hybridmoln hos Försvarsmakten 16
5 Förslag på molntjänster 17
5.1 OpenStack 17
5.1.1 Säkerhet i Openstack 18
5.2 VMware Vcloud 18
5.2.1 Säkerhet i VMware Vcloud 18
5.2.2 Federala risk- och befogenhetsprogrammet (FedRAMP) 19
5.2.3 Akten om federal informationssäkerhetshantering (FISMA) 19
5.2.4 Standard 27001:2005/27001:2013 19
5.3 Ekonomi 19
6 Test av OpenStack/Devstack 21
7 Analys 23
8 Slutsats och framtida arbeten 25
8.1 Slutsatser 25
8.2 Begränsande faktorer 26
8.3 Framtida arbeten 26
8.4 Reflektioner 26
Referenser 27
Bilaga A: Försvarsmaktens verksamhetsanalys för IT-system 30
Bilaga B: Installation av Oracle VirtualBox, Ubuntu och Openstack/devstack 31

Lista på figurer

Figur 2-1: Informationssäkerhetens tre pelare 7
Figur 5-1: Uppbyggnaden av Openstacks molntjänst[1]..... 17
Figur 6-1: Lyckad installation av Devstack 21
Figur 6-2: Instrumentbrädan som ger en överblick av molnet. 22

Lista på tabeller

Tabell 2-1: Sju av Försvarsmakten och säkerhetspolisens (SÄPO) säkerhetsfunktioner för IT-system. 9
Tabell 2-2: Försvarsmaktens krav på skyddande av uppgifter inom den egna verksamheten. 10
Tabell 3-1: Samtliga stegen i forskningsprocessen 13

Lista på akronymer och förkortningar

CRASH	Clean-Slate design of Resilient, Adaptive, Secure Hosts
DARPA	(Unites States of America) Defence Advanced Research Projects Agency
DHCP	Dynamic Host Configuration Protocol
FOI	Totalförsvarets forskningsinstitut
IaaS	Infrastructure as a Service
MRC	Mission-oriented Resilient Clouds
MUST	Militära underrättelse- och säkerhetstjänsten
NAT	Network Address Translation
NIST	National Institute of Standards and Technology
OSL	Offentlighets- och sekretesslagen
PaaS	Platform as a Service
PuL	Personuppgiftslagen
RAM	Random Access Memory
SaaS	Software as a Service
SAP	Systems, Applications and Products
SÄPO	Säkerhetspolisen
TCP	Transmission Control Protocol
VPN	Virtual Private Network
UDP	User Datagram Protocol

1 Introduktion

"Den Svenska Försvarsmakten existerar för att skydda Sverige och för att bibehålla nationens frihet. Försvarsmakten är Sveriges verktyg för att skydda Sveriges gemensamma värderingar, skydda Sveriges gränser och att vara en del av de uppdrag som bibehåller och främjar fred." [1]

Detta kapitel innehåller en kort bakgrund till detta arbete, en problemdefinition, syfte med arbetet, vilka mål som satts upp, vilken metod som använts under arbetets gång, avgränsningar och slutligen vilken struktur rapporten har.

1.1 Bakgrund

Molntjänster har ett brett användändningområde och kan bland annat användas för att lagra information på ett smidigt och eventuellt lönsamt sätt. En uppdatering av Försvarsmaktens IT-system skulle inte bara innebära smidigare hantering av information utan även en mer lönsam lagring.

En implementation skulle kunna använda sig av en extern ”kontrakterare” som erbjuder Försvarsmakten lagringsutrymme i sitt moln. I detta fall skulle hemlighetsstämplad information behöva krypteras mot obehörig åtkomst till information från kontrakterarens moln. Om PUL ska uppfyllas kan en lösning vara att kryptera de delar av informationen som PUL ställer integritetskrav på varefter den resterande informationen kan lämnas okrypterad.

För att hålla information hemlig internt kan flera mindre nät användas där alla sektioner av Försvarsmakten eller alla behörighetsgrupper i Försvarsmakten har sitt eget moln.

Försvarsmakten kan gynnas av att använda sig av en tredje part för molnlagring då detta kan vara ett lönsamt alternativ. Eftersom underhåll av molnet inte nödvändigtvis behöver skötas av Försvarsmakten och endast användas vid behov.

1.2 Problemdefinition

Ett scenario byggs upp där Försvarsmakten har som mål att utveckla ett molnbaserat system som är anpassat till den egna verksamheten. Här finns det många aspekter som en eventuell implementation måste ta hänsyn till. En av de större aspekterna är säkerhetsaspekten, detta eftersom att ett molnbaserat IT-system inom Försvarsmakten måste ha stort fokus på säkerheten. Ett molnbaserat system har många fördelar, bland annat när det gäller ekonomi och skalbarhet. Dock kan detta endast implementeras om säkerhetsnivåerna uppnår de krav militära underättelse- och säkerhetstjänsten (MUST) ställer på Försvarsmaktens IT-system.

Försvarsmakten bedriver en rad olika verksamheter med varierande säkerhetsnivåer när det kommer till informationshantering. I detta arbete vill vi därför undersöka hur ett molnbaserat system kan implementeras på olika sätt för att uppfylla de olika säkerhetskraven.

1.3 Syfte

Syftet med detta projekt är att undersöka några sätt hur Försvarsmakten eventuellt skulle kunna implementera moln för den egna verksamheten utan att behöva kompromissa de säkerhetsföreskrifter och regler som informationshanteringen styrs utav. Samtidigt som man måste tänka på att upprätthålla och bevara den befintliga säkerhetsnivån på Försvarsmakten, måste man även försöka maximera den nytta en eventuell implementation av molntjänster skulle kunna ge.

I denna rapport undersöks även vilka ekonomiska följder införandet av molntjänster på Försvarsmakten skulle medföra och huruvida den ekonomiska aspekten är en tillräckligt stor anledning för att gå vidare med implementationen

Påverkan på det administrativa arbetet skulle kunna vara positivt i samband med ett eventuellt införandet av molntjänster hos Försvarsmakten. Dels för att det ständiga underhållet av de lokala servrarna skulle ersättas med tjänster där underhållsansvaret helt läggs över på tjänsteleverantörerna, men även för att hanteringen och de generella arbetet med lagring skulle kunna bli smidigare. Även denna aspekt kommer därför att undersökas vidare, hur kan man förbättra det administrativa arbetet i samband med införandet av moln.

1.4 Mål

Detta arbete har som mål att ta fram och analysera idéer för hur Försvarsmakten på ett effektivt sätt skulle kunna implementera olika typer av molnbaserade system inom den egna organisationen. Målen har skrivits i punktform nedan efter att ha delats upp i delmål:

- Framtagning av förslag för hur Försvarsmakten kan använda sig av moln inom den egna organisationen.
- Analys av molnteknologin för att se på vilka sätt en sådan skulle kunna anpassas efter Försvarsmaktens verksamhet
- Presentera och analysera tjänster från två olika molntjänstleverantörer
- Sätta upp ett av molnen från molntjänstleverantörerna som presenteras för att få en idé om hur en implementation kan tänkas bli.

1.5 Undersökningsmetod

För att genomföra detta arbete valde vi att använda oss av fyra steg som är beskrivna nedan:

1. Definiera problemet
2. Samla relevant information
3. Ta fram lösningsförslag
4. Analysera lösningsförslag

Arbetets metod kommer att struktureras på så sätt att vi inledningsvis definierar problemet, följt av att vi samlar information om området, varefter en analys görs på den samlade informationen. Efter analysen formuleras en tänkbar lösning till problemet.

1.6 Avgränsningar

Att testa och ta fram ett verkligt system tar lång tid och kräver även tillgång till dessa system, vilket det inte finns tidsmässigt utrymme för inom ramen för detta arbete. Därför kommer detta arbete att fokusera på hur en eventuell implementation av ett molnsystem hos Försvarsmakten skulle kunna se ut rent teoretiskt.

1.7 Rapportens disposition

Kapitel 2 – Presentation av relevant bakgrund för att förenkla förståelsen för moln och information om Försvarsmakten i dagsläget. I denna del presenteras även relaterande arbeten inom områden.

Kapitel 3 – Detta kapitel beskriver ingående vilken metodologi och vilka metoder som användes under arbetets gång.

Kapitel 4 – Detta kapitel ger förslag på hur en implementation kan ske med avseende på hybridmoln, publika moln samt privatmoln. För varje molntyp ges exempel på vad Försvarsmakten bör tänka på .

Kapitel 5 – I detta kapitel beskrivs två olika molntjänster; OpenStacks molntjänst och en myndighetsanpassad tjänst från VMware. Beskrivningen sker med ett fokus på ekonomi och säkerhet.

Kapitel 6 – Detta kapitel visar hur det såg ut vid den egna uppsättningen av OpenStack/DevStack.

Kapitel 7 – I detta kapitel analyseras samtliga lösningsförslag som tagits fram.

Kapitel 8 – Detta kapitel innehåller diskussioner om begränsningar i arbetet, framtida arbeten, diskussion om etiska aspekter och hur vårt slutresultat stämmer överens med våra mål för arbetet.

2 Bakgrund

Detta kapitel lyfter fram och presenterar relevant bakgrund för att skapa en grundläggande förståelse för moln, säkerhet inom moln och delar av Försvarsmaktens nuvarande IT-system samt krav för nya IT-system inom organisationen. I slutet av kapitlet redovisas relevanta arbeten inom områden och avslutas sedan med en sammanfattning.

2.1 Vad är molnet?

Att hitta en entydig definition på vad molnet är kan vara svårt. Efter flera sökningar har vi fått fram två förklaringar som hjälper oss att klargöra ordets betydelse.

Nationalencyklopedin hade följande definition: “molnet, datamolnet, datormolnet, externt serverutrymme för datortjänster som är tillgängliga via Internet från enskilda datorer”. Exempel på datortjänster som kan användas inom molnet är datafilslagring, applikationer och program. När dessa datortjänster körs på Internet utgör de tillsammans så kallade molntjänster [2].

National Institute of Standards and Technology (NIST) beskrev molnet som ett tillträde till en delad samling av olika typer av datorresurser som vid behov tillåts tillgång till med minimala insatser från användaren och tjänsteleverantören. Datorresurser som skulle kunna tänkas användas är nätverk, servrar, lagring, tjänster och applikationer [3].

En allmän förståelse för hur datalagring och informationshantering, hanterad internt/lokalt inte är det mest lönsamma, smidiga eller effektiva alternativet har gjort att man ständigt letar efter moderniserade alternativ till informationshantering som sänker kostnader och administrativ arbete.

Eftersom molntjänster kan erbjuda ett lönsamt och smidigt system för hantering av data är det idag ett område som placerar sig allt högre på företags och organisationers agenda runt om i världen.

Moln som helhet består huvudsakligen av fyra olika typer: privat, publikt, “samhälls-” och hybridmoln. Dessutom finns det tre olika servicemodeller för moln. Dessa består av Mjukvara-som-service (SaaS), Infrastruktur-som-service (IaaS) och Platform-som-service (PaaS) [3].

2.1.1 Typer av moln

Enligt NIST finns det fyra olika typer av moln[4]. Dessa fyra olika modeller presenteras nedan.

Privat moln Ett privat moln är endast avsett för användning av en specifik organisation. Det är endast denna organisation som ska ha tillgång till molnet och det som lagras i det. Molnet kan styras av organisationen eller en tredje part eller en kombination av dessa.

Publikt moln Publika moln och dess infrastruktur kan vara tillgängligt för allmänheten eller en större industriell organisation. Molnet kan ägas, styras och hanteras av exempelvis ett företag, organisation, myndighet, skola eller en blandning av dessa.

“Samhällsmoln” I ett så kallat ”samhällsmoln” kan en bestämd grupp som till exempel består av flera organisationer använda sig av molnet. Denna typen av moln används av organisationer med samma krav molnets uppbyggnad, exempelvis när det gäller säkerhetskrav eller policies. Ett samhällsmoln styrs och hanteras av en tredje part, en eller flera organisationer inom den bestämda gruppen eller en kombination av dessa.

Hybridmoln Ett hybridmoln består av en sammansättning av två eller flera publika, privata eller samhällsmoln. Infrastrukturen är därför anpassad beroende på vilka kombinationer som används. De respektive molnen kvarhåller sina unika egenskaper och tillsammans ses dessa kombinationer som en enhet som utgör ett hybridmoln.

2.1.2 Servicemodeller för moln

Det finns tre servicemodeller för moln:

Mjukvara-som-service (SaaS) Mjukvara-som-service är en form av on-demand mjukvara som man via ett moln kan få tillgång till. Denna typ a moln används oftast av stora organisationer för att få användning av applikationer från externa parter[4]. För att få tillgång till de applikationer som molnet erbjuder måste man därför ha en etablerad nätverksuppkoppling, exempel är hur en större del av denna sorts applikationer nås via webbläsare. Applikationerna används bara vid behov, exempel på SaaS är Facebook och google som man får åtkomst till via internet. Ägarna av SaaS produkterna är de som tar hand om underhållningen och utvecklingen av produkten vilket innebär att organisationer som använder sig av SaaS inte behöver lägga ner tid och resurser på drift av applikationer [5].

Plattform-som-service (PaaS) Plattform-som-service är en tjänst som erbjuder organisationer och kunder en plattform för utveckling och användning av applikationer. Det detta medför är att organisationer undgår arbete med underhåll och drift av infrastrukturer tillhörande sina applikationer [6]. PaaS låter organisationer (bl.a., det finns två typer av PaaS) och kunder ta hand om applikationens utveckling och konfiguration, men lämnar lagrings-, nätverks- och serverproblemen till molntjänsteleverantören [5].

Infrastruktur-som-service (IaaS) Infrastruktur-som-service är en typ av moln som erbjuder tjänster i form av virtuell hårdvara. Detta kan till exempel vara virtuellt serverutrymme, nätverksuppkoppling eller ip adresser [7]. Leverantören av IaaS molntjänsten ansvarar för hårdvaruresurser som man drar från en mängd servrar och nätverk som oftast är placerade i flera datacenter. Klienten får tillgång till de virtuella hårdvarudelarna för att kunna bygga och utveckla sina IT-plattformar [5].

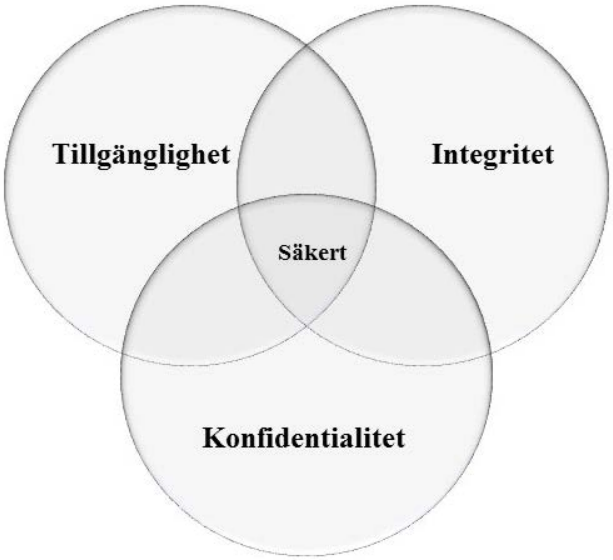
2.2 Säkerhet

Konfidentialitet, Integritet, Tillgänglighet (engelska; ”Confidentiality, Integrity, Availability (C.I.A)”), utgör informationsäkerhetens tre pelare som går att se i Figur 2-1. [8]. För att information/data ska kunna anses vara “säkert” måste dessa tre pelare uppfyllas samtidigt, den kortfattade innebörden av de tre pelarna är följande:

Konfidentialitet *“Är hjärtat för alla säkerhetspolicies för informationsystem. Säkerhetspolicies är den grupp regler som, givet identifierade subjekt och objekt, avgör huruvida ett givet subjekt kan få tillgång till ett specifikt objekt” [8]*

Integritet *“Är kvaliteten på information som visar hur nära informationen representerar verkligheten. T.ex, hur nära representerar ditt CV dig själv)” [8]*

Tillgänglighet *“Information ges till användare med rätt behörighet när den är efterfrågad eller nödvändig.” [8]*



Figur 2-1: Informationssäkerhetens tre pelare

2.2.1 Säkerhet i molnet

Om man ser på molntjänster ur ett datalagringsperspektiv kan det i många fall vara ett mycket säkrare alternativ för datalagring än lagring på lokala servrar eller maskiner [9]. Trots detta finns det ändå en del brister i molnsystem som måste hanteras och bearbetas för att kunna göra molnsystem tillräckligt säkra för Försvarsmakten. Eftersom moln inte bara används för lagring av data utan även för processering (PaaS) och infrastruktur (IaaS) är det viktigt att man beaktar säkerhetsriskerna med alla dessa punkter i åtanke.

Det första som händer när molntjänster implementeras är att ansvaret för säkerheten blir en delad börda för både molntjänsteleverantören och molnanvändaren [5]. Det som är problematiskt med detta är att användarens krav på säkerhet måste vara uppfyllda på leverantörens sida och om

de inte är det så faller själva ansvaret för ett eventuellt säkerhetsfel på användaren (om man utgår ifrån hur de flesta kontrakt mellan användare och leverantörer är uppbyggda) [5].

Den största säkerhetsfrågan som troligen uppstår hos en användare av molntjänster är huruvida den information och data man hanterar via molnet är tillgänglig för alla andra som använder sig av samma leverantör [10].

För att bekämpa denna osäkerhet finns det en hel del åtgärder. En åtgärd som kan utföras på många olika sätt, är att använda sig av krypteringsmetoder på den data som ska hanteras av ett moln från en tredje part. På detta sätt ser man till att datan inte kan tolkas även om obehöriga får tillgång till den. Ett annat exempel på vad man kan göra är att använda sig av det publika tredjepartsmolnet, endast för hantering av publik data som inte kräver någon specifik form av behörighetsgrad. Den konfidentiella datan kan man istället hantera lokalt i ett privat moln eller på lokala servrar.

2.3 Försvarsmakten

Med runt 20000 anställda är Försvarsmakten en av Sveriges största myndigheter. Riksdagen och regeringen styr Försvarsmaktens uppgiftsområden och hur verksamheten bedrivs. Totalt har myndigheten fyra huvuduppgifter som består av att:

1. Skydda och försvara Sverige vid intrång från främmande makt
2. Avvisa främmande makter om Sveriges gränser kränks
3. Hjälpa till med olika stödinsatser vid olyckor och katastrofer
4. Verka för fred och säkerhet i världen genom att exempelvis skicka fredsbevarande styrkor till utsatta områden i världen.

Myndigheten består av flera mindre enheter som kan delas in i förband, skolor, centrum och enheter [11].

2.3.1 Försvarsmaktens nuvarande system

Försvarsmakten har som mål att under 2016 utveckla det vanliga kontorsnätet så att information upp till säkerhetsklassen hemlig/restricted ska kunna hanteras inom det. I det vanliga kontorsnät använder sig Försvarsmakten av SharePoint som samarbetsverktyg och för expeditionshantering [12]. SharePoint är en webbapplikation som utvecklats av Microsoft. Programet möjliggör hantering och lagring av information på datorer. SharePoint går att få tillgång till från vilken dator som helst inom Försvarsmakten, det enda kravet är att de finns tillgång till någon typ av webbläsare som Google Chrome, Internet Explorer eller Mozilla Firefox. Leverantören erbjuder sedan olika typer av tilläggstjänster och varianter av SharePoint [13].

För tid- och lönehantering använder sig Försvarsmakten av det SAP-baserade systemet PRIO som även hanterar en viss del av försvarslogistiken [12].

2.3.2 Implementation av nya IT-system i Försvarsmakten

Vid en implementation av ett nytt IT-system inom Försvarsmakten är det enligt Försvarsmaktens handbok för IT-säkerhet [14] av stor vikt att göra en noggrann analys av säkerhetsmålsättningarna. Dessa säkerhetsmålsättningar är uppdelade i verksamhetsanalys, regelverksanalys, säkerhetsanalys och en IT-säkerhets-specifikation.

Verksamhetsanalys En verksamhetsanalys är en beskrivning av den verksamhet som IT-systemet ska stödja samt en beskrivning av de uppgifter som systemet ska behandla. I denna del definieras krav på tillgänglighet utifrån de krav som den specifika verksamheten har.

Regelverksanalys Regelverksanalysen går ut på att beskriva och definiera de regler, lagar och författningar som IT-systemet måste följa.

Säkerhetsanalys Denna analys går ut på att identifiera hot och risker med IT-system och hur hanteringen av dessa bör utföras.

IT-säkerhets-specifikation En systembeskrivning och en kravlista med säkerhetsfunktioner tas fram. Säkerhetskraven tolkas och en beskrivning av hur de uppfylls görs.

2.3.3 Säkerhetsfunktioner

Inom Försvarsmakten anpassas IT-systemen efter vilken informationssäkerhetsklass som är den högsta inom det använda systemet. I Tabell 2-1 presenteras sju säkerhetsfunktioner som bygger på en eller flera funktioner för att Försvarsmakten ska bevara de krav som finns på säkerhet inom sina IT-system. Dessa funktioner har tagits fram med hjälp av de regler som styr hur ett IT-system bör skyddas [14].

Tabell 2-1: Sju av Försvarsmakten och säkerhetspolisens (SÄPO) säkerhetsfunktioner för IT-system.

	Säkerhetsfunktion
1	Behörighetskontroll
2	Säkerhetsloggning
3	Skydd mot röjande signal
4	Skydd mot obehörig avlyssning
5	Intrångsskydd
6	Intrångsdetektering
7	Skydd mot skadlig kod

Enligt Försvarsmaktens handbok kan ett tillräckligt skydd inte åstadkommas endast med hjälp av dessa sju säkerhetsfunktioner. Ett skydd för ett IT-system kräver att fler åtgärder för skydd identifieras och lyfts fram [14]. Dessa skyddsåtgärder tas fram och dokumenteras med hjälp av de punkter som finns tillgängliga i Tabell 2-1.

2.3.4 Skyddsaspekter

I säkerhetstjänstens handbok för informationssäkerhet ställs krav på vilka sätt information bör skyddas. De skyddsaspekter som Försvarsmakten tar upp presenteras i Tabell 2-2.

Tabell 2-2: Försvarsmaktens krav på skyddande av uppgifter inom den egna verksamheten.

Skyddsaspekt	Krav
1	Uppgifter ska inte finnas tillgängliga eller avslöjas för obehöriga personer.
2	Uppgifter inte ändras avsiktligt eller oavsiktligt.
3	Uppgifter finns tillgängliga i förväntad omfattning.
4	Att händelser som är säkerhetspåverkande går att härleda till identifierade användare.

2.4 Informationssäkerhetsklasser hos Försvarsmakten

Nedan presenteras informationassäkerhetsklasser som hämtats från Försvarsmaktens handbook för informationssäkerhet [14].

2.4.1 Hemlig/Top secret

Denna klassen har den högsta säkerhetsnivån inom Försvarsmakten. Dessa uppgifter bör behandlas med ett omfattande skydd för att begränsa åtkomsten för oberhöriga. Anledningen till detta är att infomationen som har denna klassificering vid röjande kan medföra stora risker för rikets säkerhet och förhållanden till andra stater eller organisationer. Dessa handligar har av utländska myndigheter eller organisationer klassats som “top secret”.

2.4.2 Hemlig/Secret

Detta är den näst högsta säkerhetsnivån inom Försvarsmakten. Information som inte fått en specifierad klass men ändå kan ses som hemlig placeras i hemlig/secret. Informationen inom denna säkerhetsklass kan vid röjande orsaka omfattande risker för rikets säkerhet och förhållanden till andra stater eller organisationer. Dessa handligar har av utländska myndigheter eller organisationer klassats som “secret”.

2.4.3 Hemlig/Confidential

I den tredje högsta säkerhetsnivån inom Försvarsmakten placeras informationen som vid röjande kan medföra en liten men inte betydelselös risk för rikets säkerhet och förhållanden till andra stater eller organisationer. Dessa handlingar har av utländska myndigheter eller organisationer klassats som “confidential”.

2.4.4 Hemlig/Restricted

I den lägsta av alla säkerhetklasser som är hemliga samlas information som vid röjande kan medföra en marginell risk för rikets säkerhet och förhållanden till andra stater eller organisationer. Av utländska myndiheter klassas dessa handlingar som “restricted”.

2.4.5 Ej sekretess

I denna nivå samlas all information som inte styrs av några bestämelser i offentlighets- och sekretesslagen (OSL). Detta betyder dock inte att dessa uppgifter inte kan få en högre säkerhetsklass. Genom att kombinera flera uppgifter som kan ha olika säkerhetsklasser och på så sätt få fram ett innehåll i dessa som kan ge upphov till någon typ av skada som nämns i säkerhetsklasserna ovan kan dessa uppgifter tillsammans få en ny säkerhetsklass [15].

2.5 Relaterade arbeten

The (United States of America) Defense Advanced Research Projects Agency (DARPA) som är en del av det amerikanska försvarsdepartementet har utfört ett flertal olika typer av program som är relevanta inom området för denna rapport. Nedan nämns två av dessa program.

2.5.1 Nystartad design av elastiska, anpassningsbara och säkra värdar (CRASH)

DARPA har i programet CRASH haft som mål att ta fram nya tekniker och system som effektivt kan skydda och förbättra olika typer av datorsystems motståndskraft mot cyberattacker. Dessa tekniker består av ökat skydd mot cyberattacker, anpassning efter en eventuell cyberattack som möjliggör fortsatt användning av viktiga delar av datorsystemet, att lära sig från tidigare attacker och på så sätt göra det möjligt att motverka dessa i framtiden och automatisk reparation efter en lyckad cyberattack [16]. Detta arbete är relevant då det behövs som grund för att använda sig av uppdragsorienterade elastiska moln (MRC) som strävar efter att ta fram nya och säkra möjligheter för användande av moln.

2.5.2 Uppdragsorienterade elastiska moln (MRC)

Programet MRC, som även det utvecklats av DARPA, har som mål att ta fram nya möjligheter när det kommer till ett säkert användande av moln. MRC är ett tilläggsprogram till det tidigare programet CRASH och fungerar som ett hjälpmedel till det. Säkerhetsaspekterna inom MRC involverar ett effektivt och kollektivt skydd med hjälp av flera värdar, igenkänning av attacker och nya tekniker för ett skapande av anpassningsbart skydd för attacker [17]. Arbetet är relevant då säkerhetslösningar som presenteras även skulle kunna vara tänkbara lösningar för Försvarsmakten i en eventuell implementering av moln.

2.5.3 Säkerhet för molnbaserade tjänster

I ett tidigare examensarbete skriver Sabrina Ali Tandra och Saruwal Islam Rizivi om säkerhet för moln generellt och för olika typer av molnbaserade tjänster [18]. Säkerheten är en viktig aspekt för Försvarsmakten. Därför är en grundläggande förståelse för säkerhet inom moln en viktig del för detta arbete.

2.5.4 Molnet – möjligheter och begränsningar

Totalförsvarets forskningsinstitut (FOI) har i en rapport skrivit om vilka möjligheter och begränsningar som finns med molnet. Rapporten ger en grundläggande bild av vad ett moln är, vilka funktioner som finns tillgängliga inom det och vilka risker som finns rent affärsmässigt och tekniskt [19]. Detta arbete visar vilken information Försvarsmakten tidigare har tagit fram om moln.

2.6 Sammanfattning av bakgrund

Molnet är en teknologi som potentiellt kan ge användaren goda möjligheter för en mera effektiv och sparsam användning och hantering av data och information. Teknologin har ett brett användningsområde och kan bland annat användas för informationslagring och processering. Detta skulle kunna användas av Försvarsmakten men eftersom att organisationen har tydliga krav och processer för införandet av nya IT-system måste en eventuell implementering vara väl anpassad efter dessa krav. En stor del av kraven ställs på säkerheten som molnet måste uppfylla. Att ta fram ett nytt IT-system för Försvarsmakten är därför en uppgift som noggrant måste tas fram och bearbetas.

3 Metod

I detta kapitel kommer de metoder som användes för detta arbete att beskrivas. Efter att ha övervägt användningen av den valda metoden och både kvalitativa och kvantitativa metoder kom vi fram till att de två sistnämnda inte skulle vara lämpliga för denna typen av arbete.

En kvantitativ metod kräver tid och resurser som detta arbetes omfattning inte tillåter. Denna metod förutsätter att vi implementerar en lösning eller tar fram kvatifierbar data, statistik och resultat från tidigare lösningar. Detta är något som är svårt att utföra inom ämnesområdet med de begränsningar arbetet har.

Vi kommer därför att utföra en typ av litteraturstudie som används som grund för analyser och val av lösningsmetoder.

3.1 Forskningsprocess

Detta arbete kommer att delas upp i de fyra stegen som redovisas i Tabell 3-1.

Tabell 3-1: Samtliga stegen i forskningsprocessen

Steg	Syfte
1.	Definiera problemet
2.	Insamling av lämplig information
3.	Ta fram lösningsförslag för varje del
4.	Analysera samtliga lösningsförslag

3.1.1 Steg 1: Definiera problemet

I det första steget av denna metod är huvudmålet att ta fram ett tydligt och väldefinierat problem. Definitionen till framtagningen av lösningen måste under arbetets gång utvecklas och förbättras från sitt första stadie, som inte är omfattande nog för att vara tillfredställande. För att kunna göra detta är det viktigt att identifiera behovet av lösningen och skapa en djupare förståelse för problemet. Efter detta är det viktigt att kunna formulera och uttrycka problemet på ett korrekt sätt.

När problemet är färdigformulerat blir nästa steg att sätta upp mål och kriterier som ska uppnås för att nå ett eventuellt slutmål. Exempel på kriterierna kan vara att: ha en låg ekonomisk kostnad, uppnå en viss grad av skalbarhet eller uppfylla vissa typer av säkerhetskrav.

3.1.2 Steg 2: Insamling av lämplig information

Det andra steget består av att samla in information som är relevant för det problem som formulerades i steget innan. Detta steget är viktigt eftersom att det kan spela en stor roll i problemdefinitionens utveckling. Relevant information kan avslöja fakta inom området som skulle kunna ändra de initiala uppfattningarna angående problemet.

3.1.3 Steg 3: Framtagning av lösningsförslag

I steg tre vidareutvecklas den befintliga informationen för att möjliggöra en lösning. Genom att sammanställa den insamlade informationen går det att få en överblick av området och utifrån detta framställa lösningar. I detta steg kan ett kreativt och i vissa fall risktagande tänkande vara till stor nytta i jakten på innovation och nytänkande.

3.1.4 Steg 4: Analys och val av lösningsförslag

När framtagningen av lösningsförslag är gjord måste dessa analyseras och i vissa fall måste ett val göras för att ta fram det mest lämpliga alternativet för att lösa det specifika problemet. Denna del går alltså ut på att presentera och diskutera lösningsförslagen som togs fram i steget innan.

3.2 Insamling av information

Insamlad information har främst hämtats från böcker och med hjälp av sökningar på internet. Sökmotorn som KTH bibliotek erbjuder har använts.

4 En eventuell implementation hos Försvarsmakten

Detta kapitel handlar om egenskaper hos de tre olika molntyperna publik, privat och hybrid och vad Försvarsmakten bör tänka på för respektive typ om en eventuell implementation skulle bli aktuell.

4.1 Publikt moln hos Försvarsmakten

I denna del presenteras några delar och säkerhetsfunktioner inom användningen av publika moln som Försvarsmakten kan ha nytta av vid en eventuell implementation.

4.1.1 Användningen av tredje part

Något som Försvarsmakten måste ta hänsyn till vid användningen av ett publikt moln är att en tredje part kan vara involverad. Det finns tredje parter som erbjuder publika molntjänster mot en betalning beroende på vilka tjänster som köps. En ekonomisk fördel med detta är att användaren då endast betalar en kostnad vid användning. Det kan uppstå en del problem vid användning av en tredje parts leverantör. Ett av dessa kan vara hanteringen av sekretessbelagd information. Om exempelvis information som rekryteringen inom Försvarsmakten måste skyddas av personuppgiftslagen (PuL) så är inte användningen av tjänster via en tredje part att föredra. Detta eftersom att informationen som lagras i molnet kan spridas till obehöriga parter. Ytterligare en nackdel med anvädningen av en tredje parts tjänster är att ansvaret för informationssäkerheten delas mellan molnleverantören och användaren.

4.1.2 Kryptering

Det molnanvändaren på egen hand kan göra för att garantera informationens säkerhet är att kryptera informationen så att obehöriga inte kan tolka informationen även om de har fått tillgång till den. Denna metod skulle kunna användas av Försvarsmakten för att uppfylla PuL. Därför kan kryptering erbjuda ett sätt för Försvarsmakten att även hantera hemlig information i ett publikt moln. Med hjälp av kryptering går det att uppnå integritet och säkerhet inom molnet[20]. Två funktioner som kan kan användas som hjälpmedel för att uppnå detta är att använda sig av nyckel-hashade funktioner och vaktposter som beskrivs i “Providing Security and Integrity for Data Stored In Cloud Storage”[20].

4.1.3 Nyckel-hashade funktioner

Innan informationen lagras i molnet så processeras den på användarens sida. Det man gör är att man krypterar informationen vilket skapar en hash och dessutom genereras en hash-nyckel och ett hashvärde. Hashen som skapades placeras sedan i molnet. Dessa redskap hjälper till att kontrollera så att integriteten är intakt, det vill säga att ingen data i filen har ändrats sedan den lagrades i molnet. För att kontrollera att integriteten hållits skickas hash-nyckeln till molnet som i sin tur använder nyckeln på den lagrade hashen. När detta är gjort skickas ett hash-värde som sedan går att jämföra med det tidigare genererade hash-värdet för att se om de är identiska. Om dessa värden skiljer sig åt går det att säga att integriteten är kompromenterad.

Ett problem med denna metod är bördan som den skapar på användarens sida gällande lagring av data. Då stora hash-värden och nycklar för varje fil måste lagras lokalt kräver det stora lagringsutrymmen hos användaren. Om denna funktion används av en stor organisation, exempelvis Försvarsmakten, kan påfrestningen för de lokala lagringsutrymmena bli stort[20].

4.1.4 Vaktposter

Detta säkerhetsskydd går ut på att för all information som lagras i molnet placeras vaktposter ut i datan. Vaktposterna är slumpmässigt utlagda block i filen vars positioner kan hjälpa till att avgöra huruvida en fils integritet är intakt. Vaktposternas positioner samlas hos användaren som sedan kan se om filen har ändrats genom att jämföra vaktposternas nuvarande positionering med den ursprungliga. Även denna metod ställer krav på datalagring som kan bli stora vid användning inom större organisationer.

4.2 Privat moln hos Försvarsmakten

En implementation av ett privat moln inom Försvarsmakten är ett alternativ som skulle innebära att en kryptering av information, som skydd mot tredje parter, inte skulle vara nödvändig. Detta betyder inte att någon form av kryptering inom organisationen inte behövs. Ett privat moln skulle bara användas av Försvarsmakten, vilket skulle bidra till att det inte är något krav på att använda sig av en tredje part för hanteringen av molnet. Det privata molnet skulle eventuellt kunna tas hand om internt på Försvarsmakten. Säkerhetsåtgärderna skulle vara fokuserade på de olika behörighetsnivåerna istället för hot från utsidan. En av fördelarna med moln är förbättrad skalbarhet, denna fördel riskerar man att gå miste om ifall man implementerar ett privat moln som styrs internt. Detta eftersom att underhållet av ett sådant moln skulle innebära mycket mer arbete för Försvarsmakten. Det alternativ som finns, för att implementera ett privat moln och fortfarande uppnå en bättre skalbarhet, är att implementera ett privat moln som styrs av en tredje part. Men då uppstår problemet med den delade arbetsbördan igen, den tredje parten måste tillgodose Försvarsmaktens krav på säkerhet och accesser. Ett privat moln skulle förbättra säkerheten för den information som har en högre hemlighetsnivå då molnet bara används inom organisationen.

4.3 Hybridmoln hos Försvarsmakten

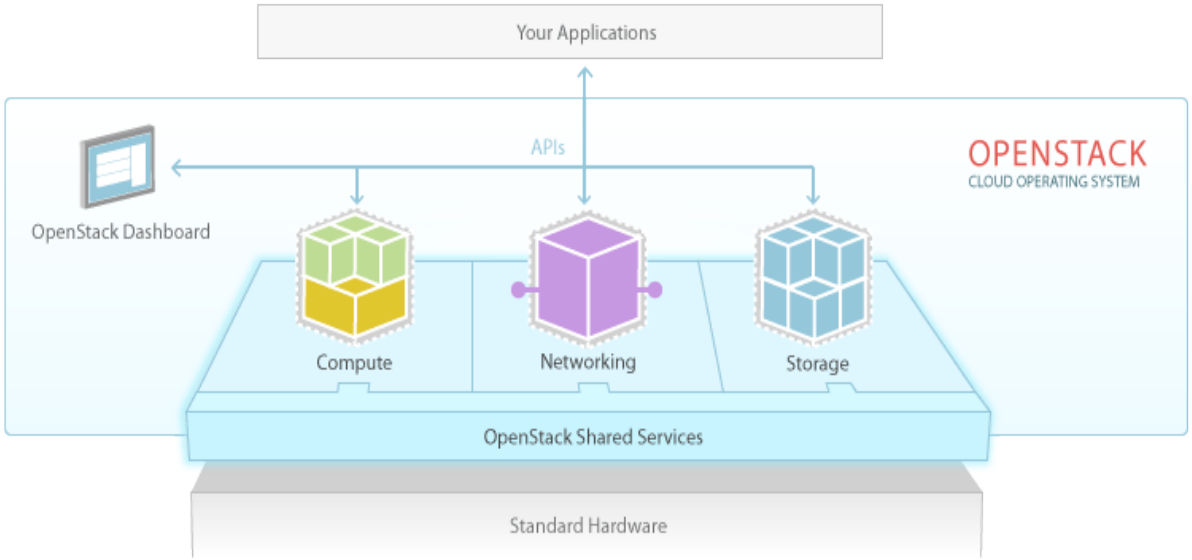
Försvarsmakten är en organisation med en rad olika verksamheter, med olika säkerhetsföreskrifter. Detta är något som är viktigt att tänka på när man vill implementera nya IT-system, så effektivt som möjligt, inom organisationen. De publika och privata molnen beskrivna ovan är användbara för olika delar av Försvarsmaktens verksamhet, men en av de två metoderna kan inte enskilt implementeras för att omfatta hela verksamheten. Hybridmoln kan ge Försvarsmakten möjligheten att kombinera privata moln med publika moln samt servrar och få de att fungera tillsammans sömlöst, som en kombinerad plattform[21]. Detta betyder att Förvsarsmakten skulle kunna utnyttja fördelarna med både publika moln och privatmoln. Högre säkerhet kan uppnås genom användning av det privata molnet eller dedicerade servrar, samtidigt som molnets skalbarhet kan utnyttjas i form av t.ex. det publika molnet[21].

5 Förslag på molntjänster

Det finns ett flertal företag som erbjuder olika former av molntjänster. Två av dessa har valts ut som förslag och redovisas nedan.

5.1 OpenStack

OpenStack är ett molnbaserat operativsystem, med öppen källkod, som ger möjligheten att skapa privata och publika moln. Genom OpenStacks datacenter kontrolleras mängder av resurser i form av processering, lagring och infrastruktur. Alla dessa resurser är applikationsprogrammeringsgränssnitt, eller API, drivna. resurserna hanteras via systemets instrumentbräda (dashboard), som är ett grafiskt gränssnitt, en web-applikation, som för administratörer möjliggör ett sätt att få tillgång till, underhålla och automatisera de molnbaserade tjänsterna [22]. I Figur 5-1 presenteras hur hela uppbyggnaden av OpenStacks molntjänst ser ut.



Figur 5-1: **Uppbyggnaden av Openstacks molntjänst[1]**

OpenStack har hand om stora nätverk av virtuella maskiner. Detta gör det möjligt för dem att erbjuda företag och organisationer processeringsresurser vid behov. Systemet är väldigt flexibelt tack vare sin förmåga att integrera med tredjeparts teknologier och de “odefinierade” hårdvaru- och mjukvarukraven som den ställer på organisationerna som den ska integreras med[22].

OpenStack fokuserar huvudsakligen på två typer av datalagring, objektlagring och blocklagring. Blocklagring går ut på att lagra jämnstora block av data, vilket skiljer sig från det mest vanliga lagringsalternativet, fillagring, som går ut på att lagra filer. Blocklagring kan vara en effektiv lagringsmetod med avseende på processeringen då hanteringen av stora block är enklare än hanteringen av mindre “enheter” [23]. Objektlagring går inte ut på att lagra varken filer eller block av data, utan på att lagra objekt. I denna typen av lagring går det inte att bara skriva till en fil utan all data i ett objekt skrivs till samtidigt [23].

Systemet erbjuder även nätverksresurser för hantering av nätverk och ip-adresser[22].

5.1.1 Säkerhet i Openstack

OpenStack är ett system med öppen källkod, detta faktum är något som skapar nya säkerhetsfrågor utöver de frågor som en allmän implementation av molnsystem skapar. Den öppna källkoden innebär att systemets källkod är tillgänglig för allmänheten [24]. Trots att OpenStack är ett av de mer poPuLära alternativen för företag som vill implementera molntjänster i sin verksamhet, har systemet en del brister i sin säkerhet [25].

Projekt i OpenStack får man tillgång till först efter man har blivit autentiserad som användare. Autentisering sker med ett personligt användarnamn och lösenord. OpenStack saknar en viktig komponent för säkerheten i sin lösenordshantering, nämligen specificerade krav på lösenordskomplexitet. Systemet tillåter användare att använda sig av lösenord utan några krav på komplexiteten hos lösenorden, vilket leder till att många lösenord inte är tillräckligt “starka” för att kunna anses vara säkra. Detta leder till en större risk för att attacker, där lösenord blir hackade, blir lyckade. En annan Svaghet gällande lösenorden är att de i stor omfattning är lagrade i klartext, något som leder till en väldigt uppenbar säkerhetsbrist [26].

Systemet saknar även adekvata behörighetskontroller som hjälper till att granska huruvida hemlighetsstämplade filer fås åtkomst till av användare med rätt behörighetsnivå. Dessa hemlighetsstämplade filer kan innehålla extremt känslig information såsom lösenord. Om accessen till denna typen av filer inte hanteras på ett tillräckligt säkert sätt kan följderna bli stora och svåra [26].

En annan säkerhetsbrist är det faktum att OpenStack inte använder sig av kryptering på filer då de flyttas inom molnet. Detta medför att filer som flyttas inom molnet är sårbara/tillgänliga på samma sätt som de lösenord som sparas i klartext [26].

5.2 VMware Vcloud

VMware vCloud erbjuder flera olika alternativ när det kommer till moln. En av dessa tjänster, VMware vCloud Myndighetsservice (VMware vCloud Government Service), är anpassad till myndigheter. Denna tjänst består av en platform för ett hybridmoln vilket gör det till PaaS-tjänst. I grund och botten bygger platformen på WMwares Vsphere som är en server virtualisering. Det finns två olika modeller för denna myndighetstjänst. Den första är ett dedikerat moln och det andra är ett virtuellt privat moln. Med denna platform kan Amerikanska myndigheter på ett säkert sätt förlänga sina egna datacenter så att de fungerar med molnet[27]. På sin hemsida är informationen och tillgängligheten endast riktad till Amerikanska myndigheter och det framgår inte hur tjänsten förhåller sig till andra myndigheter i världen. Alternativet finns dock endast tillgängligt vid besök på den Amerikanska hemsidan.

För de som väljer att teckna avtal VMware vCloud Myndighetsservice finns det ett grundutbud av vilka tilläggstjänster som ingår. Dessa tilläggstjänster består av processering, lagring, bandbredd och publika IP-adresser, brandväggsalternativ, lastutjämning för trafik mellan olika nätverks gränssnitt, översättning av IP-adresser mellan nätverk (NAT), tilldelning av IP-adresser för datorer (DHCP) och en VPN-tjänst [28].

5.2.1 Säkerhet i VMware Vcloud

Till skillnad från OpenStack så har WMware inte någon öppen källkod i sin tjänst för myndighetsservice. Istället bygger tjänsten på ytterligare en part, Carpathia, som tillsammans med WMware erbjuder detta alternativ [27]

På sin hemsida presenterar VMware olika certifikat, säkerhetsklasificeringar och regleringar som uppfylls vid användandet av WMware Vcloud. Några av dessa är: Federala risk- och befogenhetsprogrammet (FedRAMP) , Federal informationsprocesserings Standard (FIPS) 140-2, Internationella standardiseringsorganisationen (ISO) 27001:2005 [27].

5.2.2 Federala risk- och befogenhetsprogrammet (FedRAMP)

I Amerikanska finns ett myndighets baserat program, FedRAMP, som har som uppgift att tillföra en standardiserad mall för säkerhetsutvärderingar, befogenhetskontroller och övervakning av molnbaserade tjänster och produkter. Själva säkerhetsutvärderingen som utförs i FedRAMP programmet använder sig av krav som utgår från akten om federal informationssäkerhetshantering (FISMA) [29].

5.2.3 Akten om federal informationssäkerhetshantering (FISMA)

FISMA är en akt som ställer krav på Amerikanska fedarala myndigheter att utveckla, dokumentera och implementera program som garanterar säkerhet för information samt informationssystemen som används inom myndigheterna [30].

5.2.4 Standard 27001:2005/27001:2013

Internationella standardiseringsorganisationen och internationella elektrotekniska komissionen (ISO/IEC) har tillsammans tagit fram standarder som innehåller specifikationer för produkter, tjänster och system. Dessa standarder används för att säkerställa kvalitet, säkerhet och effektivitet inom specifika områden[31].WMware uppfyller ISO/IEC 27001:2005 som för tillfället har blivit reviderad till ISO/IEC 27001:2013[32][27]. Denna standard innehåller krav på hur hanteringssystem för informationssäkerhet inom organisationer ska implementeras, etableras, underhållas och förbättras. Standarden innehåller även krav på bedömningar och hantering av olika säkerhetsrisker vad gäller informationssäkerhet [33].

5.3 Ekonomi

När det kommer till ekonomiska frågor och molntjänster finns det ett flertal olika perspektiv som Försvarsmakten skulle ha en fördel av. En av de större fördelarna är att organisationer kan anpassa tjänsterna efter eget användande. Det går då att endast betala för de tjänster som används vilket skulle kunna sänka kostnader då man inte betalar för ett paket med tjänster där vissa tjänster går oanvända.

En annan fördel är att kostnader för systemadministratörer sänks eftersom att ett molndatacenter gör det möjligt för en enskild administratör att hantera fler servrar än i ett traditionellt datacenter [34]. Detta märks framförallt vid användning av publika moln då ansvaret för underhåll, uppdatering av system och liknande uppgifter sköts av tjänsteleverantören. Detta minskar behovet av en intern IT-avdelning som sköter liknande typer av uppgifter inom organisationen [35].

Genom att investera i moln som har en kapacitet som överskrider kapaciteten hos de interna servrarna inom en organisation, kan organisationen spara en del pengar. Den ökade kapaciteten för organisationen innebär kortare processeringstider och snabbare utförda uppgifter. Eftersom att molnleverantörer erbjuder tjänster med bestämda priser per tidsenhet blir kostnader för snabba användningar av moln låga, detta kan alltså för organisationen potentiellt innebära snabbare arbete och ett sparande av pengar[36].

Vid ett lyckat användande av molnstjänster försvinner en stor del av belastningen på den interna IT-utrustningen då delar av data och applikationer körs via molnet istället. Detta leder i sin tur till att organisationers IT-utrustning blir mer långlivad och behovet av en uppdatering av IT-utrustningen inte blir lika återkommande. Ett resultat av detta blir att organisationers budget, i lika stor utsträckning, inte går åt att uppdatera utrustning [36].

En annan fördel med moln är att man kan få tillgång till nya resurser snabbt. Detta är inte alltid fallet när man jobbar med interna servrar inom ett företag, då nya resurser kräver installation och man ofta måste vänta på leverans av resurser. Den snabba tillgången till nya resurser innebär att man flexibelt kan anpassa molnet efter verksamhetens behov och slutföra uppgifter och mål på kortare tid. Att slutföra projekt och uppgifter snabbare kan innebära ett sparande av finansiella medel, speciellt i samband med användning av moln, där kostnader har en tendens att öka linjärt med tid [36].

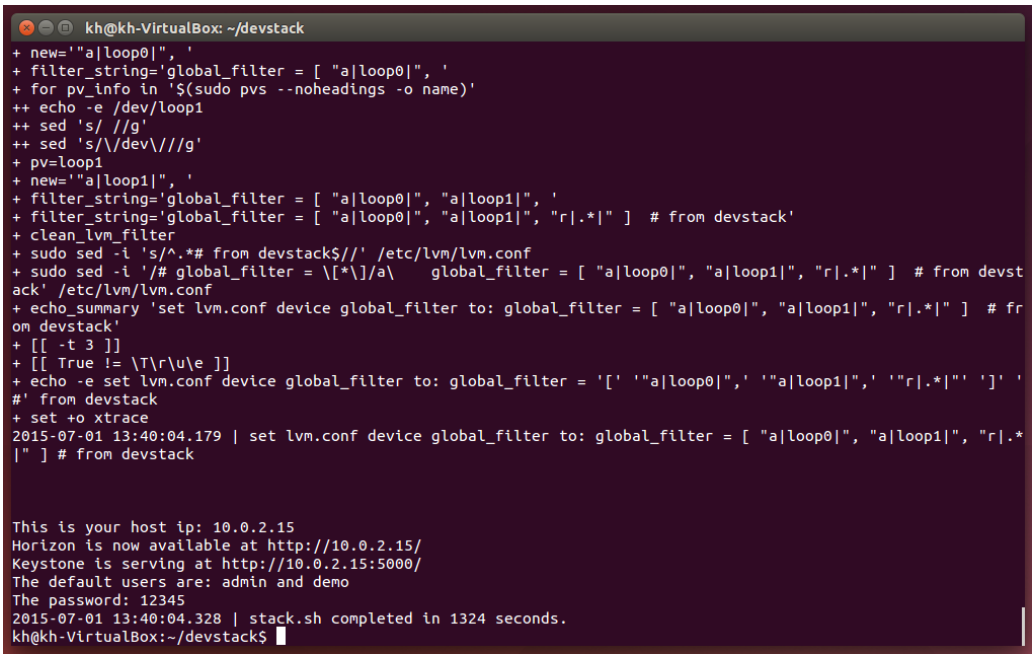
Moln utgår, i de flesta fall, från specifika mätvärden i sin prismodell såsom lagringsutrymme, RAM, bandbredd, användningstid och så vidare [37]. Detta kan hjälpa organisationer att på enklare sätt hantera sin budget och balansera den med behovet av IT-resurser. Molntjänster har oftast fullständigt definierade prismodeller och med hjälp av dessa kan man enklare förutspå och planera kostnader och ekonomiska satsningar inom IT-systemen [37]. Lokala servrars kostnader kan vara svårare att förutspå om man jämför med molnkostnader. Ett exempel på detta är om till exempel servrarna kraschar, kostnader för att åtgärda detta kan bli höga. Kostnader kan även bli höga om ett moln kraschar, men en sådan kostnad faller oftast på molntjänsteleverantören.

Vid användningen av ett publikt moln betalas det endast en konstnad för användningen av molnet och dess resurser. Ett privat moln genererar utöver kostnader för användning även konstander för underhåll av resurser och tjänster. Den viktiga egenskapen hos moln när det kommer till ekonomi är skalbarheten. Molntjänster kan anpassas utefter användarens behov. Hos publika moln är lättare att styra skalbarheten än vad det är i privata moln. Detta eftersom att det vid användningen av ett privat moln kräver att användaren köper in fast del av tjänsten som grund, även fast denna del inte utnyttjas fullständigt. Detta problem slipper användaren med publika moln då behovet styr inköpet av tjänster.

6 Test av OpenStack/Devstack

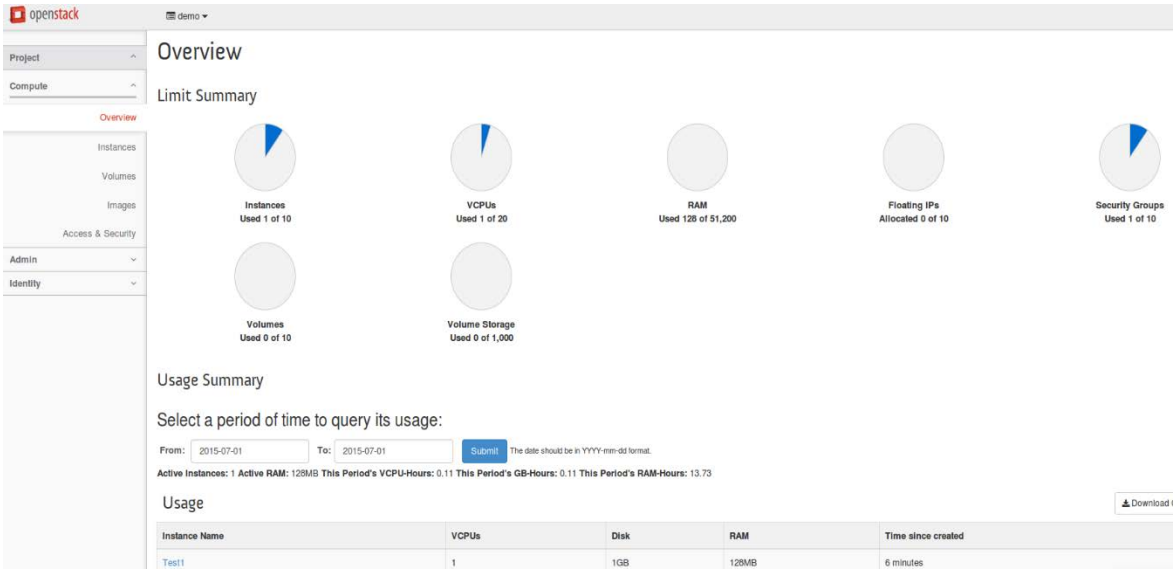
För att få en klarare bild av hur en implementation av OpenStack skulle kunna se ut för Försvarsmakten valde vi att sätta upp detta. En virtuell maskin med operativsystemet Ubuntu användes för installationen. En fullständig förklaring av installationen går att hitta i bilaga B.

Efter att ha hämtat hem Devstack, tagit fram rätt inställningar och kört kommandot ”./stack.sh” påbörjades installationen. I Figur 6-1 går det att se att installationen är lyckad och att tjänsten är uppsatt och redo för användning. Det framgår tydligt vilken adress som används för att få tillgång till Horizon som är en instrumentbräda där olika tjänster kan hanteras.



Figur 6-1: **Lyckad installation av Devstack**

Figur 6-2 visar hur instrumentbrädan ”horizon” ser ut efter att vi loggat in med användarnamn och lösenord. I figuren framgår det vilka tjänster som används och i hur stor utsträckning. Det finns begränsningar på de flesta tjänsterna, ett exempel på detta är hur den maximala storleken på RAM-minnet är 51,200 Megabyte (Mb) (vårt användande uppgår till 128 Mb).



Figur 6-2: Instrumentbrädan som ger en överblick av molnet.

OpenStack kan via instrumentbrädan anpassas så att bara en viss typ av trafik kan passera genom en specifik instans i molnet. Detta möjliggörs med hjälp av regler för dataöverföringsprotokollen ”Transmission Control Protocol” (TCP) och ”User Datagram Protocol” (UDP), detta kan ses i Bilaga-B. Detta är en bra funktion som Försvarsmakten skulle kunna använda sig av för att på ett enkelt sätt endast tillåta trafik från den egna organisationen.

OpenStack uppfyller inte flera av de säkerhetskrav som Försvarsmakten ställer, detta går att se då antalet säkerhetsfunktioner inom tjänsten är begränsade. Detta innebär att Försvarsmakten, vid en eventuell implementation, främst skulle kunna använda sig av detta för hanteringen av ej sekretessbelagd information. Sekretessbelagd information skulle eventuellt kunna hanteras via OpenStacks tjänster ifall en lämplig kryptering av informationen gjordes i förhand.

7 Analys

Efter att ha utfört detta arbete har förslag på lämpliga implementeringsmetoder hittats. Dessa metoder är väldigt olika och det är viktigt att ha en klar bild av vad som skall åstadkommas innan ett beslut fattas. De metoder som redovisats i detta arbete har olika styrkor och svagheter, vilket gör dem lämpliga för olika typer av verksamheter inom Försvarsmakten.

Om Försvarsmakten endast skulle implementera ett privat moln skulle detta ge en hel del fördelar när det kommer till säkerhet. Detta eftersom att ett privat moln skulle erbjuda en möjlighet för Försvarsmakten att skydda sin verksamhet tack vare att ett sådant moln skulle kunna styras av Försvarsmakten om de själva var värden. Något att tänka på vid val av denna lösningen är att kostnaderna kan bli högre än vid till exempel användningen av en leverantör. Detta på grund av att Försvarsmakten själva måste stå för underhåll och drift av molnet samt för kostnaderna för införandet av molnet.

Ett annat alternativ är att använda sig av en molntjänstleverantör. Denna lösning kan i många fall leda till en ekonomisk fördel gentemot ett självkonstruerat privatmoln, då kostnader för underhåll, drift och uppsättandet av molnet undviks. Ett problem som kan uppstå när en molntjänsteleverantör ska väljas är att leverantören måste kunna uppfylla de krav på säkerhet som Försvarsmakten har på sin verksamhet. Ett exempel på detta är de två molntjänstleverantörerna Openstack och VMware som erbjuder två olika former av informationssäkerhet. Molnstjänsteleverantören och Försvarsmakten måste tillsammans dela på säkerhetsansvaret. Ansvaret på molnleverantören kan därför bli därför omfattande, då Försvarsmakten har höga krav på säkerheten inom de egna IT-systemen. I kapitel 5 presenteras VMware och tjänsten för myndigheter i USA. Vcloud molnet som VMware erbjuder är ett moln som lever upp till flera erkända krav och standarder för IT-säkerhet för amerikanska myndigheter. WMware är ett exempel på en leverantör som potentiellt skulle kunna möta Försvarsmaktens säkerhetskrav. Men att göra ett definitivt antagande om huruvida VMware skulle vara en lösning är svårt då tjänsten de erbjuder är anpassad för de Amerikanska myndigheterna.

Kapitel 5 presenterar även molntjänsten som OpenStack erbjuder. Många av Försvarsmaktens säkerhetskrav och skydd mot attacker är inte standardiserade i OpenStacks molntjänster. Detta innebär att Försvarsmakten skulle behöva implementera egna skydd och säkerhetsfunktioner för att kunna använda sig av OpenStack. Försvarsmakten får alltså uppgiften att säkerställa molnanvändningen, förutsatt att OpenStack används för att behandla sekretessbelagd information. Om tjänsten endast används för hantering av ej sekretessbelagd information elimineras detta problem och fördelarna med OpenStacks välutvecklade molntjänst kan då utnyttjas.

Tjänsterna är effektiva för olika användningsområden. För att en molnimplementation ska kunna omfatta Försvarsmaktens samtliga verksamheter är en kombination av de olika lösningsförslagen troligtvis en bra lösning. Med hybridmoln går det att kombinera de olika molntyperna och utnyttja deras olika användningsområden så att Försvarsmaktens informationshantering, som helhet, blir effektiviserad.

Det som är viktigt att beakta vid analys av dessa resultat är att lösningsförslagen bara är teoretiska. För att Försvarsmakten ska kunna välja ett eller flera av lösningsförslagen krävs det noggranna och utförliga tester av de olika tjänsterna som föreslagits.

8 Slutsats och framtida arbeten

I detta kapitel presenteras arbetets slutsatser och eventuella framtida arbeten inom området.

8.1 Slutsatser

De målen som sattes upp för detta arbete uppnåddes. Flera olika förslag på hur Försvarsmakten kan använda sig av moln inom den egna organisationen togs fram. De förslag vi tog fram är teoretiska och har inte kunnat testas praktiskt. Eftersom att de kan finnas skillnader mellan teoretiska lösningar och deras praktiska tillämpning blir det svårt att säga att de lösningar vi kommit fram till under detta arbete är de mest lämpliga för Försvarsmakten.

Det andra målet var att analysera molnteknologin och se hur denna skulle kunna anpassas efter Försvarsmaktens verksamhet. Detta mål medförde en uppdelning i två deluppgifter. Den första deluppgiften var att analysera molnteknologin. För att möjliggöra detta krävdes en grundläggande förståelse för molnteknologin vilket medförde att en stor del av bakgrunden gick ut på att förklara denna teknologi. Den andra deluppgiften från detta mål var att analysera Försvarsmaktens verksamhet. För att kunna anpassa det vi lärde oss om molnteknologin till Försvarsmakten krävdes en tydlig bild av verksamheten. Detta bidrog till att även denna del blev en stor del av bakgrunden.

Målet om att presentera och analysera tjänster från två olika molnleverantören hade ett blandat resultat. Valet av molnleverantörer gjordes till viss del utan någon form av motivering. Detta var ett resultat av den begränsade information angående Försvarsmaktens verksamhet och nuvarande system samt våra tids- och kunskapsbegränsningar inom området. Det kan finnas alternativ på molntjänsleverantörer som passar Försvarsmaktens verksamhet bättre än de två vi valde att analysera i detta arbete. Samtidigt finns det många goda aspekter med molnleverantörer vi valde att analysera. Openstack som är en av de större molnleverantörerna erbjuder goda möjligheter för egen utveckling av tjänsterna. VMware har erfarenhet av arbete med amerikanska myndigheter och om en liknande typ av molntjänst skulle kunna anpassas efter den svenska Försvarsmaktens krav på IT-system skulle denna erfarenhet vara till nytta.

Målet om att testa en av tjänsterna som föreslagits i arbetet var till en början svårt då uppsättningen krävde kunskaper inom Linux. Efter många försök installerades tjänsten från OpenStack/DevStack på ett lyckat sätt. Den tydliga instrumentpanelen gav en enkel bild och överblick av tjänsten vilket underlättade hanteringen.

Under arbetets gång har vi insett att området är väldigt brett och därför skulle arbetet gynnas av en mer fokuserad och avsmalnad riktning. Delar av detta arbete har förändrats ett par gånger under arbetets gång. Exempel på detta är hur mål har strukits eller ändrats i takt med att vår kunskap inom ämnet ökat. Eftersom att vår kunskap inom området till en början var begränsad var det svårt att lägga fram klara och tydliga mål som kunde förbli oförändrade. Därför är det förslag vi kan ge till andra att tidigt lägga fram mål och riktningar som ger en tydlig bild av vad som ska göras. Det är även viktigt att själva målen är tillräckligt specifierade för att undvika att arbetsbördan blir för stor.

Om detta arbete hade utförts igen hade mer fokus lagts på att förstå Försvarsmaktens nuvarande system och deras behov av exempelvis lagringsutrymme. Detta hade gjort det lättare för oss att kalkylera exakta kostnader och att se vilka leverantörer som skulle kunna tillgodose dessa behov. En tydligare vy av de nuvarande systemen hade gjort det enklare att se vilka specifika säkerhetskrav som bör ställas på ett nytt IT-system.

8.2 Begränsande faktorer

De största begränsande faktorerna var bristen på information om Försvarsmaktens nuvarande system samt bristen på kunskap inom området. Detta medförde att vi var tvungna att ägna en stor del av tiden till att hitta relevant information och samtidigt utveckla den egna kunskapen. En annan begränsande faktor var tiden som gjorde det svårt att hinna utföra alla delar på bästa möjliga sätt. Tidsbegränsningen och bristen på information från Försvarsmakten gjorde det omöjligt att implementera en lösning som var specifikt anpassad efter Försvarsmaktens verksamheter.

8.3 Framtida arbeten

Arbetet har fortfarande en del oavklarade uppgifter. Föjande uppgifter anser vi vara intressanta att arbeta vidare med:

- Framtagning av en praktisk implementation av molnsystem för Försvarsmakten för att kunna se effekterna av ett molnsystem på organisationens verksamhet.
- Test av säkerhetsfunktioner för hantering av data/information i publika moln. Exempelvis kryptering av data/information.
- Mer detaljerad undersökning av kostnaderna av ett molnsystem inom Försvarsmakten.

De förslag vi skulle ge till de som vill följa upp detta arbete är att följa punkterna ovan. Till en början kan ett fokus läggas på de ekonomiska följderna av införandet av ett nytt system, för att avgöra huruvida det skulle vara ekonomisk gynsamt eller inte. Detta kan man sedan följa upp med tester av moln specifikt anpassade efter Försvarsmaktens verksamhet, med hjälp av verksamhetsanslysen som finns i Bilaga A. Ett annat förslag vi skulle ge är att undersöka fler molntjänsteleverantörer tidigt under arbetets gång.

8.4 Reflektioner

Det finns många möjligheter när det kommer till användningen av moln. Ett exempel på detta är användningen av moln via molntjänsteleverantörer då det går att anpassa köp av tjänster till den egna användningen. Detta är gynnsamt rent ekonomiskt då inköp endast sker efter behov. Flexibiliteten vid köp av tjänster är en annan gynnsam ekonomisk aspekt då det vid behov går att utöka och minska tjänster. Molnsystem gör det oftast möjligt för organisationer att styra sin ekonomi på ett enkelt sätt, detta med hjälp av de enkla prisplaner, som molntjänsteleverantörer erbjuder, som gör att orgnisationer i förväg enkelt kan planera sin användning utefter sina ekonomiska medel. En del kostnader undviks även då mindre utrustning krävs från användarens sida för att upprätthålla IT-systemen. Mindre utrustning betyder även mindre kostnader för drift av utrustning, därför kan kostnader för, till exempel, elektricitetskonsumtion, minska. En minskad elektricitetskonsumtion innebär inte bara mindre kostnader, utan är positiv även beroende på dess mindre miljömässig påverkan.

Ur ett socialt hållbarhetsperspektiv skulle hanteringen av ett molnsystem kunna innebära en mindre arbetsbörda varför ett molnsystem potentiellt kunna innebära en lägre arbetsbelastning för delar av personalen inom Försvarsmakten. Detta kan även få omvänd effekt att folk inom Försvarsmakten blir arbetslösa då hanteringen av systemen hanteras av molntjänstleverantören.

Referenser

[1] 'Why the Swedish Armed Forces exists', Försvarsmakten. [Online]. Tillgänglig vid: http://www.forsvarsmakten.se/en/about/areas-of-responsibilities/why-the-swedish-armed-forces-exists/. [Åtkomstdatum: 23-apr-2015]

[2] 'molnet - Uppslagsverk - NE'. [Online]. Tillgänglig vid: http://www.ne.se.focus.lib.kth.se/uppslagsverk/encyklopedi/l%C3%A5ng/molnet. [Åtkomstdatum: 24-apr-2015]

[3] Steven Shepard, 'Telecommunications Crash Course, Third Edition'. [Online]. Tillgänglig vid: http://accessengineeringlibrary.com.focus.lib.kth.se/browse/telecommunications-crash-course-third-edition/c9780071832663ch11?q=cloud+storage+vs+#c9780071832663ch11lev1sec04. [Åtkomstdatum: 24-apr-2015]

[4] P. Mell och T. Grance, 'The NIST Definition of Cloud Computing -Recommendations of the National Institute of Standards and Technology'. National Institute of Standards and Technology, sep-2011 [Online]. Tillgänglig vid: http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf. [Åtkomstdatum: 24-apr-2015]

[5] J. Carstensen, B. Golden, och J. . Morgenthal, *Cloud Computing - Assessing the Risks*, vol. 2012. Cambridgeshire: IT Governance Publishing, 17 April 2012, ISBN: 9781849283595

[6] Y. Zheng, J. Pang, J. Li, och L. Cui, 'Business Process Oriented Platform-as-a-Service Framework for Process Instances Intensive Applications', i *Parallel and Distributed Processing Symposium Workshops PhD Forum (IPDPSW), 2012 IEEE 26th International*, 2012, s. 2320–2327. DOI:10.1109/IPDPSW.2012.284

[7] N. Serrano, G. Gallardo, och J. Hernantes, 'Infrastructure as a Service and Cloud Technologies', *IEEE Softw.*, vol. 32, nr 2, s. 30–36, mar 2015. DOI:10.1109/MS.2015.43

[8] J. McCumber, 'Information systems security: A comprehensive model', i *Proceedings of the 14th National Computer Security Conference*, 1991 [Online]. Tillgänglig vid: http://trygstad.rice.iit.edu:8000/Government%20Documents/NSTISS/NSTISSI4011 Annex.rtf. [Åtkomstdatum: 22-maj-2015]

[9] F. Sabahi, 'Cloud computing security threats and responses', i *2011 IEEE 3rd International Conference on Communication Software and Networks (ICCSN)*, 2011, s. 245–249. DOI:10.1109/ICCSN.2011.6014715

[10] L. Sumter, 'Cloud Computing: Security Risk', i *Proceedings of the 48th Annual Southeast Regional Conference*, New York, NY, USA, 2010, s. 112:1–112:4 [Online]. Tillgänglig vid: http://doi.acm.org/10.1145/1900008.1900152. [Åtkomstdatum: 11-jun-2015]

[11] Försvarsmakten, 'Myndigheten - Försvarsmakten', *Myndigheten*. [Online]. Tillgänglig vid: http://www.forsvarsmakten.se/sv/om-myndigheten/vart-uppdrag/myndigheten/. [Åtkomstdatum: 24-apr-2015]

[12] Ross Tsaglidis, 'Frågor till Försvarsmakten', 31-mar-2015.

[13] Microsoft, 'Vad är SharePoint?'. [Online]. Tillgänglig vid: https://support.office.com/sv-se/article/Vad-%C3%A4r-SharePoint-97b915e6-651b-43b2-827d-fb25777f446f?ui=sv-SE&rs=sv-SE&ad=SE. [Åtkomstdatum: 30-apr-2015]

[14] Försvarsmakten, 'Handbok Försvarsmaktens säkerhetstjänst, Informationssäkerhet'. 2013 [Online]. Tillgänglig vid: http://www.forsvarsmakten.se/siteassets/4-om-myndigheten/dokumentfiler/handbocker/handbok-sak-infosak-andring-1.pdf. [Åtkomstdatum: 22-maj-2015]

[15] Försvarsmakten, 'Handbok för Försvarsmaktens säkerhetstjänst, Sekretessbedömning Del A'. 2011 [Online]. Tillgänglig vid: http://www.forsvarsmakten.se/siteassets/4-om-

myndigheten/dokumentfiler/handbocker/handbok-sak-sekrbed-del-a.pdf. [Åtkomstdatum: 06-jun-2015]

[16] Defense Advanced Research Projects Agency (DARPA), 'Clean-slate design of Resilient, Adaptive, Secure Hosts (CRASH) DARPA-BAA-10-70', Arlington, jun 2010 [Online]. Tillgänglig vid: https://www.fbo.gov/utils/view?id=82f6068978da5339752c89d2f65d89ca. [Åtkomstdatum: 21-maj-2015]

[17] Defense Advanced Research Projects Agency (DARPA), Information Innovation Office (I2O), 'I2O Mission-oriented Resilient Clouds (MRC) DARPA-BAA-11-55', Arlington, jun 2011 [Online]. Tillgänglig vid: https://www.fbo.gov/utils/view?id=592b86c1bd455b12b239f695961d5354. [Åtkomstdatum: 21-maj-2015]

[18] Sabrina Ali Tandra och Sarwarul Islam Rizivi, 'Security for Cloud Based Services', Master's thesis, School of Information and Communication Technology (ICT) KTH Royal Institute of Technology, Stockholm, 2014 [Online]. Tillgänglig vid: http://kth.diva-portal.org/smash/get/diva2:691442/FULLTEXT01.pdf

[19] H. Karlzén, 'Molnet – möjligheter och begränsningar', FOI, Totalförsvarets Forskningsinstitut, Linköping, Användarrapport FOI-R--3381--SE, feb 2012 [Online]. Tillgänglig vid: http://www.foi.se/ReportFiles/foir_3381.pdf. [Åtkomstdatum: 21-maj-2015]

[20] C. S. Pawar, P. R. Patil, och S. V. Chaudhari, 'Providing security and integrity for data stored in cloud storage', i *2014 International Conference on Information Communication and Embedded Systems (ICICES)*, 2014, s. 1–5. DOI:10.1109/ICICES.2014.7033968

[21] 'Hybrid Cloud Benefits & Advantages - Rackspace'. [Online]. Tillgänglig vid: http://www.rackspace.co.uk/hybrid-hosting/benefits. [Åtkomstdatum: 16-jun-2015]

[22] Openstack.org, 'OpenStack Compute » OpenStack Open Source Cloud Computing Software'. [Online]. Tillgänglig vid: http://www.openstack.org/software/openstack-compute/. [Åtkomstdatum: 10-jun-2015]

[23] John Dickinson, 'Storage Systems Overview', *Rackspace Hosting*. [Online]. Tillgänglig vid: http://www.rackspace.com/blog/storage-systems-overview/. [Åtkomstdatum: 10-jun-2015]

[24] S. Ristov och M. Gusev, 'Security evaluation of open source clouds', i *2013 IEEE EUROCON*, 2013, s. 73–80. DOI:10.1109/EUROCON.2013.6624968

[25] S. Ristov, M. Gusev, och A. Donevski, 'Security Vulnerability Assessment of OpenStack Cloud', i *2014 Sixth International Conference on Computational Intelligence, Communication Systems and Networks (CICSyN)*, 2014, s. 95–100. DOI:10.1109/CICSyN.2014.32

[26] Hala Albaroodi, Selvakumar Manickam, och Parminder Singh, 'Critical review of Openstack Security: Issues and weaknesses', *J. Comput. Sci.*, vol. 10, nr 1, s. 23–33, 2014. DOI:10.3844/jcssp.2014.23.33

[27] WMware, 'VMware vCloud Government Service Datasheet'. 2014 [Online]. Tillgänglig vid: http://www.vmware.com/files/pdf/vcgs/vcloud-government-service-carpathia-datasheet.pdf. [Åtkomstdatum: 11-jun-2015]

[28] WMware, 'VMware vCloud Government Service Service FAQ'. 2014 [Online]. Tillgänglig vid: https://www.vmware.com/files/pdf/vcgs/vcloud-government-service-carpathia-FAQ.pdf. [Åtkomstdatum: 11-jun-2015]

[29] FedRAMP, 'Program Overview | FedRAMP', 2015. [Online]. Tillgänglig vid: https://www.fedramp.gov/about-us/about/. [Åtkomstdatum: 14-aug-2015]

[30] NIST, 'NIST.gov - Computer Security Division - Computer Security Resource Center', 31-jul-2014. [Online]. Tillgänglig vid: http://csrc.nist.gov/groups/SMA/fisma/faqs.html. [Åtkomstdatum: 14-aug-2015]

[31] ISO, 'About ISO - ISO'. [Online]. Tillgänglig vid: http://www.iso.org/iso/home/about.htm. [Åtkomstdatum: 12-jun-2015]

[32] ISO/IEC, 'ISO/IEC 27001:2005 - Information technology -- Security techniques -- Information security management systems -- Requirements'. [Online]. Tillgänglig vid: http://www.iso.org/iso/catalogue_detail?csnumber=42103. [Åtkomstdatum: 12-jun-2015]

[33] ISO/IEC, 'ISO/IEC 27001:2013(en)'. [Online]. Tillgänglig vid: https://www.iso.org/obp/ui/#iso:std:iso-iec:27001:ed-2:v1:en. [Åtkomstdatum: 12-jun-2015]

[34] Microsoft, 'THE ECONOMICS OF THE CLOUD'. nov-2010 [Online]. Tillgänglig vid: http://news.microsoft.com/download/archived/presskits/cloud/docs/the-economics-of-the-cloud.pdf. [Åtkomstdatum: 17-jun-2015]

[35] KPMG, 'Modelling the Economic Impact of Cloud Computing'. apr-2012 [Online]. Tillgänglig vid: https://www.kpmg.com/AU/en/IssuesAndInsights/ArticlesPublications/Documents/modelling-economic-impact-cloud-computing.pdf. [Åtkomstdatum: 17-jun-2015]

[36] IBM, 'IBM - Companies look to cloud to save money, build business - United States', 2010. [Online]. Tillgänglig vid: http://www.ibm.com/midmarket/us/en/article_cloud4_1209.html. [Åtkomstdatum: 17-jun-2015]

[37] Rackspace Support, 'Cloudonomics: The Economics of Cloud Computing | Knowledge Center | Rackspace Hosting', 2012. [Online]. Tillgänglig vid: http://www.rackspace.com/knowledge_center/whitepaper/cloudonomics-the-economics-of-cloud-computing. [Åtkomstdatum: 17-jun-2015]

Bilaga A: Försvarsmaktens verksamhetsanalys för IT-system

1.Vilken verksamhet ska IT-systemet stödja?

• Nationellt – internationellt?
• Fred – kris – krig?
• Kommer personal från en annan stat eller mellanfolklig organisation använda IT-systemet? 260
• Är IT-systemet avsett för användning utanför Försvarsmaktens objekt, lokaler och områden?
• Är IT-systemet avsett för distansarbete (avsnitt 15.3)?

2. Vem har ansvaret för den verksamhet som IT-systemet ska stödja?

3. Vem har ansvaret för IT-systemet och i vilken roll?

4. Vilka resurser finns för att skydda IT-systemets delar och informationen i dessa?

5. Vilka andra verksamheter eller organisationsenheter är beroende av den verksamhet som IT-systemet ska stödja?

• Vilka funktioner – vilken information? 6. Vilka (andra) verksamheter eller organisationsenheter är beroende av IT-systemet?

• Vilka funktioner – vilken information? 7. Behandlad information

• Vilken typ av information är IT-systemet avsett att behandla?

• Sekretessbedömning enligt avsnitt 14.2.1.

• Finns begränsningar av vem som får behandla uppgifter i IT-systemet?

• Finns begränsningar för personal från en annan stat eller mellanfolklig organisation att ta del av uppgifter som behandlas i IT-systemet (avsnitt 7.7)?

• Finns begränsningar (caveat) i att delge eller använda uppgifter som avses behandlas i IT-systemet (avsnitt 7.8)?

• Verksamhetens krav på tillgänglighet (avsnitt 14.2.2).

• Verksamhetens krav på riktighet. • Verksamhetens behov av nödöppning (avsnitt 7.11).

8. Kommunikation

• Vilket behov finns att överföra information på flyttbara lagringsmedier?

• Vilket behov finns att överföra information genom elektroniska kommunikationsnät?

• Övrig kommunikation till andra IT-system?

Bilaga B: Installation av Oracle VirtualBox, Ubuntu och Openstack/devstack

För att möjliggöra en installation av Ubuntu och Openstack/Devstack utan att behöva installera ett nytt operativsystem på datorn användes Oracles VirtualBox. Detta program hämtades från https://www.virtualbox.org/wiki/Downloads och i detta arbete användes version 4.3.28 för Windows hosts. Efter att programet installerats skapades en ny virtuell maskin i VirtualBox. Den virtuella maskinen hade följande inställningar:

Operativsystem:	Ubuntu 64-bitar
RAM-minne:	5051 MB
Grafikminne:	12 MB
Virtuell hårddisk:	8,0 GB

När den virtuella maskinen hade skapats användes Ubuntu Desktop som hämtades från http://www.ubuntu.com/download/desktop. Den nedladdade filen med Ubuntu Desktop lades sedan in genom att högerklicka på den virtuella maskinen i listan i Oracle VirtualBox Manager och sedan klicka på inställningar. Efter detta valdes fliken lagring och där lades filen som laddades ned från Ubuntus hemsida genom att klicka på CD-skivan vid Styrkort:IDE. När detta var gjort startades den virtuella maskinen och en installation av Ubuntu påbörjades. När denna installation var slutförd följdes guiden från Openstacks hemsida som går att hitta på http://docs.openstack.org/developer/devstack/guides/single-machine.html.

I steget där filen local.conf skulle läggas till användes först kommandot touch för att skapa filen och pico för att ändra på filens innehåll. I local.conf filen lades följande text in:

[[local|localrc]]

FLOATING_RANGE=192.168.1.224/27

FIXED_RANGE=10.11.12.0/24

FIXED_NETWORK_SIZE=256

FLAT_INTERFACE=eth0

ADMIN_PASSWORD=12345

MYSQL_PASSWORD=12345

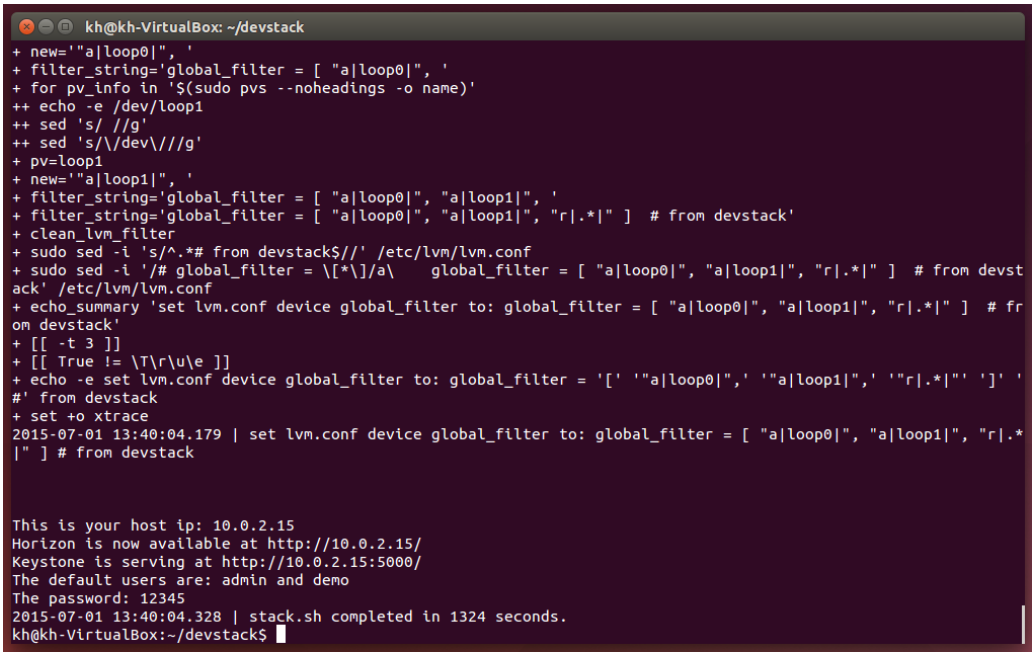
RABBIT_PASSWORD=12345

SERVICE_PASSWORD=12345

SERVICE_TOKEN=12345

ENABLED_SERVICES+=,cinder,c-api,c-vol,c-sch,c-bak

För att påbörja installationen av Openstack/Devstack skrevs "./stack.sh" i terminalen. När installationen var klar såg terminalen ut enligt bilden nedan.



På bilden går det att se vilken adress som instrumentbrädan Horizon finns tillgänglig på och sedan är det bara att öppna webbläsaren och skriva in samma adress för att komma till inloggningssidan. På inloggningssidan används de användarnamn och lösenord som även finns tillgängliga på bilden.

TRITA-ICT-EX-2015:198