

# UCN – DMAA0914

## SPECIALISERING

## VIRTUAL

Skrevet af: Kim Dam Grønhøj og Nick Reese  
Vejleder: Per Trosborg

# University College Nordjylland

Teknologi og Business

Datamatikeruddannelsen

**Hold:** Dmaa0914

**Projekt:** 4. Semesterprojekt

**Projektdeltagere:**

Kim Dam Grønhøj

Nick Reese

**Vejleder:** Per Trosborg

**Afleveringsdato:** d. 6 juni 2016

## 1 Forord

Denne rapport er udarbejdet af Kim og Nick i juni 2016, i forbindelse med et specialiserings studieprojekt på datamatiker 4. semester ved University College Nordjylland i Aalborg med vejledning af Per Trosborg og lån af hardware ressourcer af Ib Helmer Nielsen fra University College Nordjylland. Vi takker mange gange for deres vejledning og hjælp.

Projektet er henvendt til systemadministratorer, samt det er udarbejdet på at lære og forstå, hvordan vi i gruppen eventuelt bedst kan udvikle og implementere et virtuelt datacenter, der udbyder private clouds til kunder i et sikkert miljø mod uautoriseret og udefrakommende adgang. Vi vil også gerne lære og forstå de forskellige fordele og ulemper i forhold til valg af OS, software, infrastruktur og værktøjer til virtualisering, samt lære at benytte dem i praksis.

Hensigten er at vi bedre kan fremhæve, hvilke ulemper og fordele der er til høj og lav sikkerhed, hvilken betydning kan det have på performance og availability.

Rapporten indeholder, hvilke afgrænsninger vi har, kravspecifikation, teori, analyse, design af virtuel infrastruktur og valg af arkitekturer, implementering, tests og konklusion.

## 2 Indholdsfortegnelse

1	Forord.....	0
3	Indledning .....	1
3.1	Hvilke fordele er der i cloud computing?.....	1
3.1.1	Fordele og ulemper .....	1
4	Problemformulering.....	2
4.1	Afgrænsninger for projektet .....	2
4.2	Læringsmål .....	2
5	Metodebeskrivelse.....	3
5.1	Virksomhedsvejledning .....	3
6	Basis kravspecifikation .....	4
6.1	Prioritering af challenges .....	4
6.1.1	Fordele ved følgende valg .....	4
6.1.2	Ulemper ved følgende valg .....	4
6.2	Funktionelle krav.....	5
6.2.1	Systemadministrator.....	5
6.2.2	Kunde .....	5
6.3	Ikke funktionelle krav.....	6
6.3.1	Systemadministrator og udvikler .....	6
6.3.2	Kunde .....	6
6.4	Hardware .....	6
6.5	Prototyper .....	7
7	Teori .....	8
7.1	VMWare vSphere .....	8
7.1.1	Highlight vSphere applikationer og features .....	8
7.1.2	ESXI server & virtualisering .....	9
7.1.3	vSphere client.....	9
7.2	Windows server 2012 R2 datacenter - OS .....	11
7.2.1	Windows Server licens .....	11
7.2.2	Windows Server features .....	11
7.2.3	Hyper-V: Virtualisering.....	12
7.3	Middleware .....	14
7.4	Protokoller .....	14
7.4.1	Network Time Protocol (NTP) .....	14
7.4.2	User Datagram Protocol (UDP) .....	14

7.4.3	Transmission Control Protocol (TCP)	15
8	Udvikling af prototyper	16
8.1	Basal kravspecifikation	16
8.2	Implementering	16
8.3	Validering af krav	18
9	Forfin kravspecifikation	20
9.1	Funktionelle krav	20
9.1.1	Systemadministrator	20
9.1.2	Kunde	20
9.2	Ikke funktionelle krav	21
9.2.1	Systemadministrator og udvikler	21
9.2.2	Kunde	21
9.3	Hardware	21
10	Analyse	22
10.1	Analyse af IT trusler mod virksomheder	22
10.1.1	Generel trusselsvurdering for virksomheder og staten, fra Center for Cybersikkerhed	22
10.1.2	Typer af angreb	22
10.2	Konklusion af analyse	22
11	Design	23
11.1	Hardware infrastruktur	23
11.2	Virtuel infrastruktur i ESXI Server og arkitektur	24
11.2.1	Virtuel netværk	24
11.2.2	Virtuelle servers	25
12	Server 4	26
13	Server 5	27
13.2	Virtuel harddisk og backup	28
14	Final Implementering	29
14.1	Valg af hardware	29
14.2	Servere & Clients	29
14.2.1	ESXI hypervisor	29
14.2.2	Virtuel Windows Server 2012 R2 hypervisor	29
14.3	Sikkerhed	30
14.3.2	Kryptering	31
14.3.3	Isolering	31
14.3.4	IDS	31

14.3.5	Anti virus .....	32
14.4	Availability.....	32
14.4.1	Remote adgang .....	32
14.5	Performance .....	32
14.5.1	Elasticity .....	32
15	Final test.....	33
15.1	Scanning.....	33
15.2	Banner grapping.....	34
15.3	IDS detection.....	36
15.4	Uautoriseret adgang .....	37
15.4.1	VPN test.....	37
15.4.2	Firewall test.....	38
16	Studie profiler & baggrund .....	39
16.1	Nick Reese profil .....	39
16.2	Kurser .....	39
16.3	Kim Dam Grønhøj profil .....	40
16.4	Kurser .....	40
16.5	Passion .....	41
16.6	Uddannelser & kurser .....	41
17	Konklusion.....	42
18	Perspektivering .....	42
19	Procesrefleksion.....	42
20	Litteraturliste .....	42
21	Bilag.....	43
21.1	Bilag 1.....	43
21.2	Billag 2.....	44
21.3	.....	45
21.4	Bilag 3.....	45

### 3 Indledning

Vi vil i gruppen gerne udvikle en automatiseret service for kunder som søger server hosting i et sikkert datacenter. Vi vil gerne mindske at systemadministratorer eller kunder skal være fysisk tilstede i et serverrum for at opsætte nye, skallinger eller konfigurer server eller desktop maskiner.

Vi ønsker gerne at udvikle infrastrukturen virtuelt for at undgå, at vi så vidt muligt skal konfigurerer, opsætte eller tilføje fysisk hardware og infrastruktur.

Vi vil også gerne sørge for lav nedetid for kunder, uden at slukke deres server eller desktop miljø.

#### 3.1 Hvilke fordele er der i cloud computing?<sup>12</sup>

Cloud computing eller skyen er et begreb som dækker levering af software, service og tjenesteydelser via internettet, en fællesbetegnelse for anvendelse af eksempelvis SaaS (Software as a Service), PaaS (Platform as a Service) og IaaS (Infrastructure as a Service).

Cloud computing løfter flere attraktive fordele for virksomheder og slutbrugere. Tre af de vigtigste fordele ved cloud computing omfatter:

- **Self-service provisioning:** Almindeligvis kendt som cloud selvbetjening. Det er en feature, der tillader deres slutbrugere til at forsyne ressourcer til sig selv, oprette eller starte en tjeneste eller applikation uden medvirken af IT-personale eller tjenesteudbydere selv. Dette giver brugerne større frihed i, at bruge tjenester inden for grænserne fastsat af udbyderen.
- **Elasticity:** Det betyder, at IT-services automatisk får tilføjet eller reduceret hardware ressourcer under korte perioder (også kaldt dynamisk) ud fra, hvilke ressourcer IT-services bruger. *Scalability* derimod er forventet ressourcer under længere perioder, fordi man i stedet for, får garanteret ressource adgang, men kan stadig skaleres.
- **Pay per use:** En kunde betaler kun for de ressourcer og services som de har brugt, samt hvor lang tid ressourcerne er brugt.

##### 3.1.1 Fordele og ulemper

Beskrivelse	Fordele	Ulemper
<b>“Virtuel” Infrastructure as a Service (virtuel IaaS)</b> Det er en model, som tilbyder virtuelle netværk, ubegrænset private/public clouds, samt garanteret hardware ressourcer med selvbetjening..	<ul style="list-style-type: none"><li>• “Høj” elasticity og scalability af ressourcer</li><li>• Isolation af netværk</li><li>• Det er muligt at lave specielle konfigurationer</li><li>• Multiply running OS’s</li></ul>	<ul style="list-style-type: none"><li>• Høj vedligeholdelse</li><li>• Kræver høj uddannet folk</li><li>• Dyrt</li><li>• Svært at vedligeholde ressourcer over flere lokationer i verden</li></ul>
<b>PaaS (Platform as a Service)</b> Det er en model med private cloud, som kan lave flere public cloud løsninger med garanteret eller dynamisk ressourcer med selvbetjening.	<ul style="list-style-type: none"><li>• “Mellem” elasticity og scalability af ressourcer</li><li>• Mindre vedligeholdelse</li><li>• Selvvalgt OS</li><li>• Billigere</li></ul>	<ul style="list-style-type: none"><li>• Der er begrænset mulighed for at lave special konfigurationer og isolation af applikationer</li></ul>

<sup>1</sup> <https://app.pluralsight.com/player?course=cloud-computing&author=david-chappell&name=cloud-computing-m3-private&clip=0&mode=live> (25-04-2016)

<sup>2</sup> <http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf> (25-04-2016)

## 4 Problemformulering

**Hvordan kan vi designe et virtuelt datacenter med en sikker intern virtuel infrastruktur med virtuelle servere til mindre virksomheder som en service?**

For at kunne besvare dette spørgsmål, er der udarbejdet nogle **delspørgsmål**, som er listet her:

- Hvilke beslutninger ligger til grund for den valgte infrastruktur og arkitekturer?
- Hvordan sikre vi vores virtuel infrastruktur mod trafikovervågning?
- Hvordan sikre vi vores arkitektur, virtuel infrastruktur og kundernes servere mod DDoS angreb?
- Hvordan sørge vi for en sikker remote adgang til vores virtuel infrastruktur?

### 4.1 Afgrænsninger for projektet

Vores hovedfokus i disse virtuelle miljøer er, hvordan vi sikre infrastrukturens netværk mod data overvågning, uautoriseret adgang, scanning, DDoS angreb for vores egne servere.

Af hensyn til opgavens omfang har vi også kun taget fokus på følgende herunder:

- Vi har valgt kun at have fokus på ESXI og Windows Server 2012 R2 hypervisor til virtualisering.
- Under udførelse af tests og implementering har vi kun brugt en global IP, så vi er nødt til at give adgang til en NAT og DHCP server til vores kunder.
- Vi har kun 1 fysisk server. Vi prioritere derfor ikke at lave migrating af virtuelle servere med ESXI vMotion.

### 4.2 Læringsmål

- Lære at arbejde med virtualisering og forstå hvad cloud computing er og indebærer.
- Lære at bruge virtualisering værktøjer i praksis, samt opnå at opsætte vores egen virtuelle infrastruktur
- Lære at kunne analysere og penetration teste, hvilke ting i et server setup som kan være usikkert i forhold til trafikovervågning og DDoS angreb.
- Lære at kunne forhindre uautoriseret adgang til interne netværk i en virksomhed.
- Lære at forstå og bruge begreber i Windows Server 2012 R2 og VMWare ESXI 6.



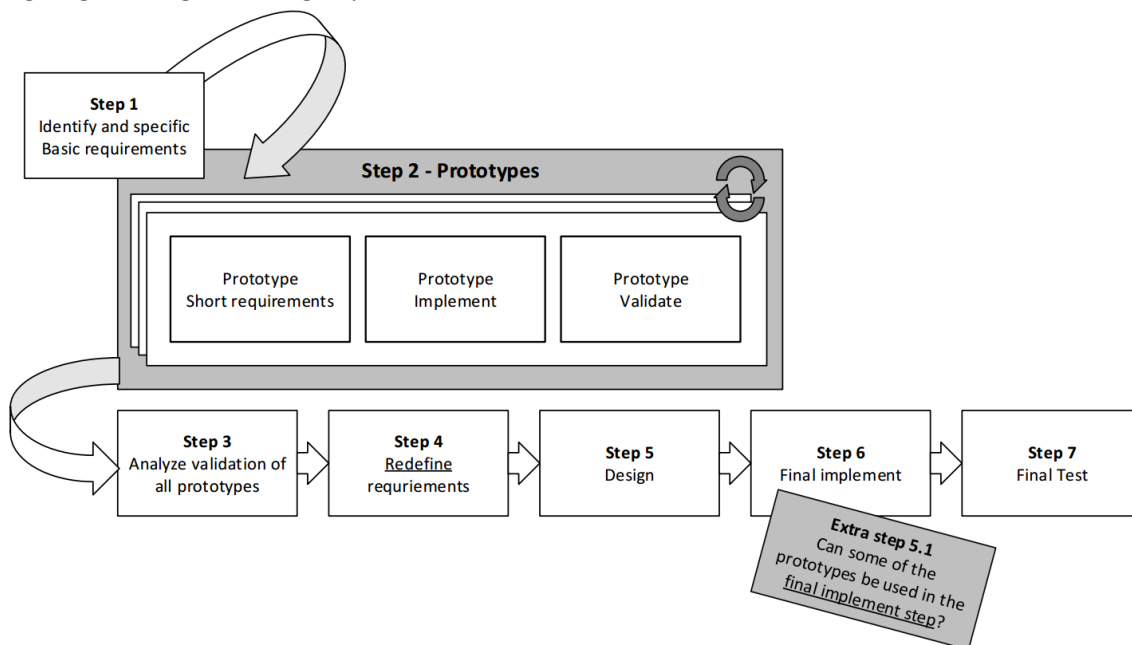
## 5 Metodebeskrivelse

Vi grab opgaven an ved delvis at benytte kanban udviklingsmetoden, for at vi kan arbejde mere agilt med et overblik over, hvilke ting vi fået lavet.

Vi har fået inspiration af følgende process modeller:

- Generelt Evolutionary development
- Throw away prototyping
- Incremental prototyping
- Evolutionary Prototyping

og valgt at bruge vores egen process model, som kan ses herunder.



Vi ser mange fordele i at mixe **specifikation, udvikling og validering** sammen, for opnå bedste mulige feedback af, hvilke ting der fungerer bedst for en systemadministrator og for en kunde. Vi er i gruppen både systemadministrator og kunde, hvilket gør det vanskeligt at kun at fokusere i et bestemt scenarie af brugertype.

Vi bruger vores egen process model, for at skabe og imødekomme den bedste kravspecifikation af det system vi gerne vil udvikle, da vi i gruppen har haft svært ved at forstå de krav vi selv stiller. Det gør, at vi hurtigt kan skabe et system som ligner noget der er færdigt.

Vi har valgt at læse meget på arkitekturene i de forskellige software fungere teoretisk og bruge den viden til at lave flere prototype integrationer af software applikationerne. Det giver os en bedre forståelse for, hvordan virtualisering fungere, og hvordan vi bedst kan implementere sikkerhed til virtuelle miljøer.

Ved implementering af prototyper er nogle prototyper bare smidt ud, hvorimod andre bevaret.

Ulempen for vores valg af process model er, at det er svært at se, hvornår udviklingen af systemet er færdigt og der sker ofte ændringer som muligvis kan ødelægge infrastrukturen eller valg arkitekturer.

De kan læses mere om evolutionær udvikling her: <http://www.robabdul.com/softwaredevelopment/software-development-cycle-for-data-management-system/> og [https://en.wikipedia.org/wiki/Software\\_prototyping](https://en.wikipedia.org/wiki/Software_prototyping)

### 5.1 Virksomhedsvejledning

Vi har også haft interview med Kasper Horsfeldt Nielsen fra Hnielsen Networks med spørgsmål om deres datacenter opsætning, og hvilke sikkerhedstiltag de har i deres setup for at reducere tiden på at udvikle servicen/systemet, da han kunne vejlede os i den rigtige retning hurtigere.

## 6 Basis kravspecifikation<sup>3 4</sup>

Vi er i gruppen meget uerfarne studerende på området med virtualisering, cloud computing og sikkerhed. Vi ligger derfor meget vægt på vores udvikling af flere prototyper til at forfine vores kravspecifikation, fordi vi har svært ved at forstå de krav vi stiller.

Kravene i dette afsnit er vægtet på ikke funktionelle krav, fordi vi vægter automatisering og sikkerhed højt i vores system.

Kravene for dette afsnit er basis krav, og disse forfines i afsnittet [Forfin kravspecifikation](#).

### 6.1 Prioritering af challenges

Vi har forskellige challenges vi gerne vil tag højde for i et hosting miljø. Vi kan ikke prioritere alle i forhold til at kunne overholde deadline til at udvikle vores system, samt det er økonomisk dyrt for en virksomhed at købe sig ind til en hosting plads, hvis alt hos os prioriteres alt for højt.

Vi har prioriteret således efter nummer:

1. Security
2. Availability
3. Concurrency
4. Scalability
5. Transparencies
6. Error handling
7. Heterogeneity
8. Openness

#### Hvorfor er security øverste?

**Vi har valgt, at sikkerhed er utrolig vigtig, fordi vi via vores service/system opbevarer store mængder fortrolige data fra flere forskellige virksomheder.**

**Vi synes også availability er vigtig i tilfælde af angreb, så vi hurtigere kan reducere skader på systemet.**

#### 6.1.1 Fordele ved følgende valg

- Mindre sandsynlighed for uautoriseret adgang.
- Mindre sandsynlighed for uautoriseret overvågning af vores kunders servers datatrafik.
- Vi kan reducere skader hurtigere.
- Som systemadministrator kan vi blive advaret hurtigere i tilfælde af angreb.
- Vi kan opnå bedre kontrol over datatrafik og ressourcer.
- Concurrency og scalability påvirkes nødvendigvis ikke.

#### 6.1.2 Ulemper ved følgende valg

- Performance reduceres.
- Availability og heterogeneity påvirkes, fordi nogle systemer kan have svært ved at snakke sammen.
- Error handling kan tage længere tid, hvis forbindelser er krypteret.
- Det kan være besværligt at få adgang til data og konfiguration.
- Data storage bliver større

<sup>3</sup> [https://en.wikipedia.org/wiki/Software\\_prototyping](https://en.wikipedia.org/wiki/Software_prototyping) (24-05-2016)

<sup>4</sup> <http://reqtest.com/requirements-blog/functional-vs-non-functional-requirements/> (25-05-2016)

## 6.2 Funktionelle krav

Vi har adskilt funktionelle krav som systemadministrator og kunde, fordi det er vigtigt at begge scenarier er specificeret. Servicen/systemet skal fungere optimalt for begge parter for at kunne have bedre kontrol og administrerer.

**Vores primær fokus er sikkerhed fra ikke funktionelle krav**, hvorimod funktionelle krav er nedprioriteret, men det har været relevant at tag med, fordi sikkerheden kan også påvirke availability og error handling til features.

**Det er vigtig, at huske disse krav herunder kun er basis krav, fordi vi havde svært ved at gennemskue, hvordan man udviklede et virtuelt datacenter som er sikkert. Disse krav forfines i afsnittet [Forfin kravspecifikation](#).**

### 6.2.1 Systemadministrator

Som systemadministrator er det vigtig at kunne overvåge og få adgang til logfiler hurtigt og nemt, samt at administrerer og konfigurer via en remote adgang.

#### 6.2.2.1 Features

- Det skal være sikkert
- Remote adgang via internet forbindelse
- Tilføj, konfigurer og slet virtuel server
- Tilføj, konfigurer og slet virtuel netværk
- Tilføj, konfigurer og slet virtual harddisk
- Tilføj, konfigurer og slet brugerrettigheder og system kontoer for egne interne systemer.
- Installere og konfigurer egne applikationer
- Ressourcestyring
- Læse og besvar support tickets

### 6.2.2 Kunde

Som kunde er det vigtigt at kunne skalere ressourcer, installere egne applikationer på en virtuel maskine og have remote adgang. Vi er kommet frem til følgende features vi ønsker til en kunde.

#### 6.2.2.2 Features

- Det skal være sikkert
- Remote adgang via internettet
- Mulighed for adgang til backup
- Adgang til kontrolpanel til konfiguration af tilknyttet virtuelle maskiner
- Tilføj support ticket til systemadministrator
- Se egne support ticket og deres status
- Mulighed for flytning af servere

### 6.3 Ikke funktionelle krav

Vi har adskilt ikke funktionelle krav som systemadministrator og kunde, fordi det er vigtigt at begge scenarier er specificeret. Servicen/systemet skal fungere optimalt og være sikkert for begge parter.

**Vores primær fokus er høj sikkerhed**, hvorimod de andre krav er nedprioriteret, men det har været relevant at tag med, fordi sikkerheden kan påvirke performance, availability og integrationskrav.

**Det er vigtig, at huske disse krav herunder kun er basis krav, fordi vi havde svært ved at gennemskue, hvordan man udviklede et virtuelt datacenter som er sikkert. Disse krav forfines i afsnittet [Forfin kravspecifikation](#).**

#### 6.3.1 Systemadministrator og udvikler

Det er vigtigt at, så meget som mulig er automatiseret, sikkert og performer godt, samt at systemadministrator ikke afhængige af bestemt en softwareleverandør.

##### 6.3.2.1 Sikkerhed, backup og overvågning

- Det skal være sikkert
- Kryptering af datatrafik ved remote adgang
- Automatisk beskyttelse mod DDOS angreb
- Automatisk backup af interne systemer og kunder

##### 6.3.2.2 Platformkrav

- Support for Windows Server 2012 R2

##### 6.3.2.3 Integrationskrav

- Mulighed for at integrere egne systemer

#### 6.3.2 Kunde

Det er vigtig for kunden at transparencies er vægtet højt, så de kan have fokus på deres forretning og udvikling og mindre vedligeholdelse af hardware.

##### 6.3.2.4 Sikkerhed, backup og overvågning

- Det skal være sikkert
- Kryptering af datatrafik ved remote adgang
- Automatisk backup af systemer og kunders virtuelle servere
- Automatisk beskyttelse mod DDOS angreb

##### 6.3.2.5 Platformkrav

- Support for Windows Server 2012 R2

##### 6.3.2.6 Elasticity

- Automatisk skalere shared ressourceforbrug for CPU, internetforbindelse og RAM

### 6.4 Hardware

Det er et krav for os, at undgå hardware vedligeholdelse, fordi dele eller alt infrastruktur skal være fleksible at flytte til forskellige datacentre over en internet forbindelse på kort tid, derfor ønsker vi et virtuel infrastruktur på et fysisk infrastruktur vedligeholde af et datacenter.

Det kræver mere software vedligeholdelse for medarbejdere og flere hardware ressourcer.

Hardware køb og hardware vedligeholdelse kan være dyrt, men det kan også være billigt, hvis man vælger at genbruge hardware hos f. eks datacenteret Hetzner i Tyskland. Vi kommer nærmere ind på følgende i vores design valg.

#### Andre krav

- Mulighed for hot plug feature i bundkort hardwaren, men er ikke et "must have"
- Billig CPU, RAM og harddisk hardware, langsigtet.

## 6.5 Prototyper

Som tidligere nævnt i [Metodebeskrivelsen](#) har vi fået inspiration af throw-away prototyping og Evolutionary Prototyping process metoderne, og brugt dem til at forfine kravspecifikationen til vores system. Dette har vi gjort, fordi vi er meget uerfarne studerende på området. Vi vil gerne lave flere prototyper, for at være sikker vores fulde kravspecifikation matcher, samt vi mener det vil hjælpe os med at designe systemet bedre. Vi er også usikre om de prototyper vi laver lever op til forventningerne.

Herunder kan du se en oversigt af de krav vi har til arbejdsprocessen af prototyperne. Vi bruger dette forløb til at kunne forfine vores kravspecifikation. Der findes i afsnittet [Udvikling af prototyper](#) selve implementering og valideringen af vores prototyper.

Prototype	Ønsket krav
<b>Hardware prototype test</b>	<ul style="list-style-type: none"><li>- Mulighed for hot plug hardware (Ikke et must)</li><li>- Billig hardware</li><li>- Det skal være muligt at lave virtuelle maskiner</li><li>- Den skal understøtte ESXI 6 eller Windows Server 2012 R2 Hyper-v</li><li>- Det skal være hurtigt og stabilt</li></ul>
<b>Windows Server 2012 R2</b> Basis features	<ul style="list-style-type: none"><li>- Beskyttelse mod password brute force</li><li>- Brugerstyring og rettigheder</li><li>- Kontrolpanel til administration af server</li><li>- Virtualisering</li></ul>
<b>ESXI Server</b> Opsætning af en virtuel server	<ul style="list-style-type: none"><li>- Virtualisering</li><li>- Ressourcetildeling</li><li>- Skalering</li><li>- Virtuel harddisk og netværk</li><li>- Remote installation af OS</li></ul>
<b>Windows Server 2016 technical preview</b> Guest hyper-v host	<ul style="list-style-type: none"><li>- Host virtuel server inde i virtuel server.</li></ul>
<b>ESXI server og konfiguration</b>	<ul style="list-style-type: none"><li>- Host virtuel server inde i virtuel server.</li></ul>
<b>Windows Server 2012 R2</b> Routing, NAT, DNS og DHCP	<ul style="list-style-type: none"><li>- Router features (Netværk opsætning)</li><li>- DNS features, så DNS opslag gøres hurtigere for kunder, samt vi ønsker bedre kontrol af DNS for kunders og interne systemer.</li></ul>
<b>Kali linux</b> Basis features	<ul style="list-style-type: none"><li>- Penetration testing</li><li>- Scanning network</li><li>- Scanning vulnerabilities</li></ul>
<b>ESXI server</b> VLAN	<ul style="list-style-type: none"><li>- Isolation af data pakker og netværk</li><li>- Automatisk drop af data pakker fra uautoriseret maskiner.</li></ul>
<b>IDS</b> OSSEC system	<ul style="list-style-type: none"><li>- Automatisk overvågning af uautoriseret adgang og angreb</li><li>- Automatisk advarsel og kategorisering</li><li>- Skal virke til Linux og Windows</li></ul>

## 7 Teori

I dette afsnit vil vi gå nærmere ind på, hvordan de software og operativsystemer vi har valgt fungere og kan bruges. Vi går også ind på begreber og softwarearkitektur.

- *“Vi synes disse emner er nødvendig at forstå, fordi det giver en bedre forståelse af vores valg, senere i rapporten, samt hvorfor komponenterne og software adskiller sig fra hinanden og hvordan de fungere.”*

### 7.1 VMWare vSphere<sup>5 6</sup>

vSphere er en suite af programmer og applikationer ligesom Microsoft Office har flere applikationer med sig.

Vi vil i dette afsnit introducere, hvilke begreber, features og applikationer som er vigtige at vide og forstå, for at kunne forstå vores valg med virtualisering for ESXI server.



#### 7.1.1 Highlight vSphere applikationer og features

- ESXI Server
  - vMotion & Storage vMotion
  - Virtual Machine File System
  - High Availability (HA)
  - Distributed Resource Scheduler (DRS)
  - Storage DRS
  - Fault Tolerance
  - Distributed Switch (VDS)
  - Hot Add
  - Host Profiles
  - Stateless Firewall
- vCenter Server management
  - vSphere Client
  - vSphere Web Client
  - Operations Management (Enterprise edition only)

---

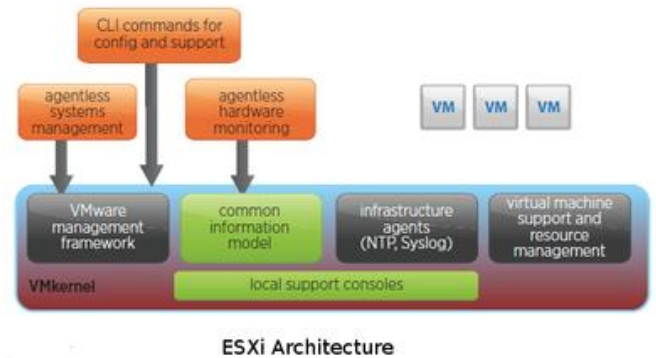
<sup>5</sup> <https://www.vmware.com/products/vsphere/compare> (02-05-2016)

<sup>6</sup> [https://www.vmware.com/pdf/vi\\_architecture\\_wp.pdf](https://www.vmware.com/pdf/vi_architecture_wp.pdf) (02-05-2016)

### 7.1.2 ESXi server & virtualisering<sup>7</sup>

ESXi er kernen som ses i Figur 1 af hypervisoren i dag. VMWare har tidligere benyttet sig af Linux kernen til at load deres hypervisor (kaldt ESX).

Fra ESX version 4.1 stoppede VMWare udviklingen af ESX og benyttede i stedet for deres egen kernel ESXi, som ikke bruger Linux kernen.



FIGUR 1

Billede:

[http://plone.4aero.com/Members/lmarzke/talks/vmug\\_esxi/esxi\\_architecture.png/view](http://plone.4aero.com/Members/lmarzke/talks/vmug_esxi/esxi_architecture.png/view)

#### 7.1.2.1 Support og kapacitet<sup>8</sup>

- ESXi supporter operativsystemer både i Windows, OS X, Linux.
- Mulighed for skalering imens virtuelle servere er online.
- Virtuel maskiner kan have op til 128 virtuel CPUs.
- Virtuel maskiner kan have op til 4 TB Ram.
- Virtual maskiner kan have op til 62 TB harddisk.
- Øget CPU effektivitet gennem støtte fra Large Receive Offload (LRO), der samler indgående TCP-pakker i en større enkelt pakke.
- Forbedre CPU virtualisering ved at eksponere flere oplysninger om CPU-arkitektur til virtuelle maskiner. Denne forbedrede CPU eksponering giver mulighed for bedre debugging, tuning og fejlfinding af operativsystemer og applikationer inden for den virtuelle maskine.
- Ny Advanced Host Controller Interface (AHCI) understøtter op til 120 enheder pr virtuel maskine.

### 7.1.3 vSphere client

vSphere klient som ses i Figur 2 er en Windows applikation du kan bruge til at remote ESXi servere ved hjælp af log ind oplysninger.

Du kan administrer en eller flere ESXi serveres med vSphere klient. er muligt, at administrer følgende via remote

- Virtuelle servere, samt remote adgang dem alle
- Virtuelle netværk og netværksopsætning
- Konfigurationer og installation af OS.
- Tilføj ressourcer og ressourcefordeling
- Storage
- Tilføj, ændre og slette moduler

Du kan ikke nødvendigvis administrer nested virtuelle servere, dog er det muligt at sætte op.



Det

FIGUR 2

Billede:

<http://www.vmwarearena.com/vsphere-6-0-download-free-esxi-6-0-license-keys/>

<sup>7</sup> <http://blogs.vmware.com/vsphere/2009/06/esxi-vs-esx-a-comparison-of-features.html> (02-05-2016)

<sup>8</sup> <http://www.vmware.com/products/esxi-and-esx/overview> (03-05-2016)

### 7.1.3.1 <sup>9</sup>Virtual switches

Ligesom fysiske switches er der virtual switches som laver forbindelse og netværk imellem komponenter og virtuelle maskiner.

vSwitchs bruger den fysiske NIC (pNIC) som ses i Figur 3 på host maskinen for at danne netværk og forbindelse til internettet som kaldes external switch. Det er også muligt at isolatorer sit eget netværk virtuelt uden en pNIC, som kaldes en internal vSwitch.

#### pNIC & uplink

pNIC i VMware som kaldes uplink adapters bruger virtuelle objekter kaldt VMNic og virtuelle adaptere for at kunne integreres med vSwitchs.

#### Teknisk forklaring

For at forklare det teknisk som ses i **Fejl!**

**Henvisningskilde ikke fundet.**, så bindes vSwitchs til en VMKernel inde i en host server. vSwitchs står til ansvar for routing af network trafik til VMKernel, VM network og Service Console (remote management). VMkernel administrer feature som vMotion, fault tolerance, network file system (NFS) og Internet small computer system interface (iSCSI). vSwitch tillader virtuelle maskiner på en ESXI server at forbinde til et fysisk netværk.

#### 7.1.3.1.1.1 <sup>10</sup>VMware virtual networking Concepts

Som standard er der et par switches og de netværk der er forbundet med dem brugt til specielle konfigurationer.

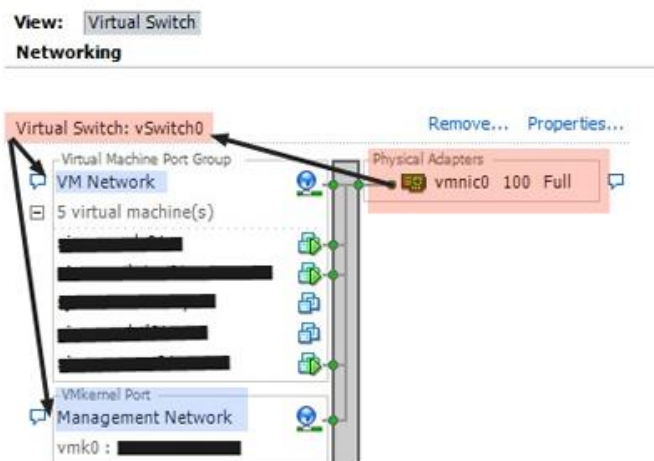
- The bridge network bruger VMnet0.
- The host-only network bruger VMnet1.
- The NAT network bruger VMnet8

#### Bridge

The bridge, det den der tillader dig at forbinde til det LAN host maskinen bruger, ved at forbinde den virtual netværks adapter i den virtuelle maskine til den fysiske Ethernet adapter i host maskinen

#### Network Address Translation (NAT)

NAT bruges til at dele en global Ip adresse på et lokalt netværk, det vil sige at flere maskiner kan komme på nettet, men ude fra vil det se ud som om de alle har samme ip adresse.



FIGUR 3

<sup>9</sup> <https://www.pluralsight.com/blog/it-ops/virtual-networking-101-understanding-vmware-networking> (07-05-2016)

<sup>10</sup> [https://www.vmware.com/files/pdf/virtual\\_networking\\_concepts.pdf](https://www.vmware.com/files/pdf/virtual_networking_concepts.pdf)



## 7.2 Windows server 2012 R2 datacenter - OS

Windows Server 2012 R2 er et populært operativt system for mindre og store virksomheder. Det er udviklet af Microsoft med fokus på at levere mange features og applikationer i en pakke.

### 7.2.1 Windows Server licens

I Windows Server verden er det vigtig at forstå, hvilke fordele og ulemper der er ved de forskellige licenser af Windows Server, fordi det kan have en økonomisk betydning for en virksomhed.

Fælles for dem alle er rigtig god dokumentation og support fra Microsoft for alle typer licenser.

Figur 4 herunder forklare, hvilke primær features og rettigheder for de forskellige licenser. Fælles for dem alle er, at virtualisering, antal af processors og antal af Windows brugere primært er forskellen.



FIGUR 4

Billede: <http://www.itgeared.com/images/content/1496-1.jpg>

### 7.2.2 Windows Server features<sup>11 12</sup>

Windows Server 2012 R2 datacenter er den fulde pakke af features, som kan løse ufattelig mange IT scenarier, dog er Microsoft bagud i virtualiseringsverden, hvor VMWare sidder på tronen, som det bedste, fordi deres styresystemer har flere features, brugervenlige og gennemtestet.

Microsoft derimod sidder godt på tronen med desktop computere og levering af avanceret server systemer til databaser, web, Office pakker, CRM, browser, netværk og server administrationen af en organisation.

De kan her se en liste af nogle de features, som findes i Windows Server 2012 R2.

- Server / client deployment
- Shared server storage, print & file services
- Health report & Windows Server Backup
- DNS, DHCP, NAT, routing
- IIS (Internet information service)
- BranchCache
- VPN, Remote web/desktop access
- Active Directory, Network policy, Access policy
- Application server
- Support for Microsoft SQL Server
- Support for PHP, C++, Python, JAVA, C#, ASP.NET
- Failover Clustering
- Powershell scripts
- Hyper-v

<sup>11</sup> [https://www.thomas-krenn.com/en/wiki/Windows\\_Server\\_2012\\_Editions\\_comparison](https://www.thomas-krenn.com/en/wiki/Windows_Server_2012_Editions_comparison) (09-05-2016)

<sup>12</sup> <https://www.vmware.com/files/pdf/vmware-vsphere-features-comparison-ch-en.pdf> (09-05-2016)

### 7.2.2.1 <sup>13</sup>Hardware requirements for Windows Server 2012 R2

Microsoft har minimum requirements for Windows Server 2012 R2 datacenter for at kunne køre. De er følgende

<b>Processor</b>	1.4 GHz 64-bit processor
<b>RAM</b>	512 MB
<b>Disk plads</b>	32 GB
<b>Network</b>	Gigabit (10/100/1000baseT) Ethernet adapter
<b>DVD drive</b>	Til at installere OS
<b>Keyboard og mus</b>	For at kunne styre OS

### 7.2.3 <sup>14</sup>Hyper-V: Virtualisering

Windows Server 2012 R2 operativsystemet indeholder rollen Hyper-V, som er en teknologi udviklet af Microsoft til virtualisering og til at administrere en eller flere maskiner, på en fysisk computer. Disse virtuelle maskiner er isoleret fra den fysiske computer, for at applikationer installeret på de virtuelle maskiner ikke kan påvirke den fysiske maskine, også kaldt Hyper-V hosten.

De virtuelle maskiner deles om, de tildelte ressourcer som Hyper-V hosten er blevet konfigureret til at må bruge, som f. eks RAM, harddisk, CPU og netværk.

Hyper-V rollen findes også som sit eget operativsystem kaldt Hyper-v Server 2012 R2, som ikke indeholder alle de features Windows Server 2012 R2 datacenter gør.

#### 7.2.3.1 <sup>15</sup>Hardware requirements

For at kunne køre Hyper-v kræver det følgende hardware

<b>Processor</b>	A 1.4 GHz 64-bit processor with hardware-assisted virtualization
<b>RAM</b>	512 MB - 4 GB
<b>Disk plads</b>	Det gør and på hvor mange virtuelle servere
<b>Network</b>	Mindst 1 network adapter

#### 7.2.3.2 Virtual Switches og netværk

I Hyper-v er det muligt at lave et internt og eksternt netværk, for de virtuelle maskiner med en eller flere virtual switches. Det er muligt at integrere disse virtuelle switches med det fysiske netværksskørt.

Du kan i tabellen herunder, se de valgmuligheder Hyper-V virtuel switches understøtter.

Navn	Funktion beskrivelse
<b>External</b>	Denne virtuelle switch er forbundet til et fysisk netværksadapter, som sørger for forbindelse mellem det fysiske netværk, Hyper-V host, og den virtuelle maskine. I denne konfiguration kan du også aktivere eller deaktivere hosten evne til at kommunikere over det valgte fysisk forbundet netværksskørt. Dette kan være nyttigt til at isolere kun VM trafik til en bestemt fysisk netværksskørt.
<b>Internal</b>	Denne virtuelle switch er ikke tilsluttet en fysisk netværksadapter, men eksisterer netværksforbindelsen mellem virtuelle maskiner og Hyper-V host.
<b>Private</b>	Denne virtuelle switch er ikke forbundet til en fysisk netværksadapter og tilslutningsmuligheder ikke eksisterer mellem virtuelle maskiner og Hyper-V host.

<sup>13</sup> [https://technet.microsoft.com/en-us/library/dn303418\(v=ws.11\).aspx](https://technet.microsoft.com/en-us/library/dn303418(v=ws.11).aspx) (15-05-2016)

<sup>14</sup> <https://technet.microsoft.com/en-us/library/mt169373.aspx> (17/3-2016)  
<https://technet.microsoft.com/library/hh831531.aspx> (17/3-2016)

<sup>15</sup> [https://technet.microsoft.com/en-us/library/jj647784\(v=ws.11\).aspx](https://technet.microsoft.com/en-us/library/jj647784(v=ws.11).aspx) (15-05-2016)

### 7.2.3.3 Hyper-v architecture<sup>16 17</sup>

Som det ses i Figur 5 er arkitekturen til Hyper-v i det første lag efter hardwaren. Det gør at Hyper host operative systemet og de virtuelle maskiner kan isoleres fra hinanden.

**VMBUS** er det vi kender fra bus i en computer, hvorimod dette er software som styrer følgende.

**VSP** står for at modtage signaler fra VSC om, hvilke ressourcer de ønsker at få tildelt og bruge.

**VSC** står for at sende signaler til VSP om, hvilke ressourcer en virtuel maskine ønsker at få tildelt og bruge. Hver virtuel maskine som kører i en **VM Worker Processe** har en VSC.

**WMI Provider** er en API service til at administrere, skalere, kontrollere ressourcer til virtuelle maskiner.

**VM Service** er client management som bruger WMI Provider API'et til at administrere virtuelle maskiner.

Hyper-V understøtter 2 typer af virtuelle maskiner som er generation 1 og generation 2.

Forskellen på disse er arkitekturen bagved.

Generation 1 virtuelle maskiner udkom ved release af Windows Server 2008, hvorimod generation 2 udkom ved release af Windows Server 2012 R2.

Den tekniske forskel på disse forklares herunder.

#### 7.2.3.3.1 Generation 1

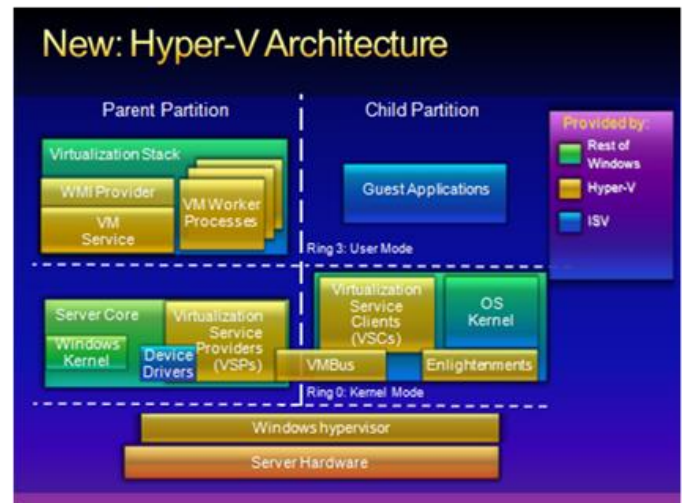
En virtuel maskine med generation 1 som ses i Figur 7 supporterer kun legacy drivers og BIOS based arkitektur. Hyper-V BIOS-based virtuel maskiner kan kun initialisere IDE controller til operativsystemet at initialisere et filsystem, som vist i Figur 7.

#### 7.2.3.3.2 Generation 2

En virtuel maskine med generation 2 som ses i Figur 8 er legacy og IDE drivers fjernet og erstattet med mulighed for at tilføje et subset af integration components, så det er muligt at load SCSI controller drivers. Det gør det muligt at boot fra en SCSI harddisk.

Følgende er også supportet i generation 2:

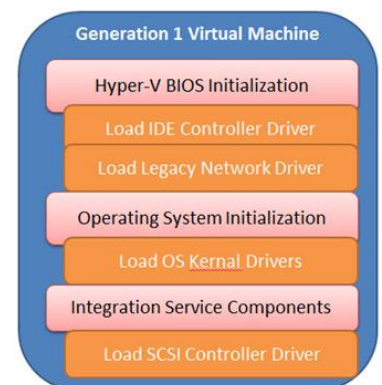
- PXE Boot – Gør det nemmere at installere et OS over netværk.
- Secure boot – beskytter mod uautoriseret firmware/devices.
- Native VMBUS Support – Integration services loader først.
- Færre drivere/devices køres i generation 2.
- Hurtigere boot time.



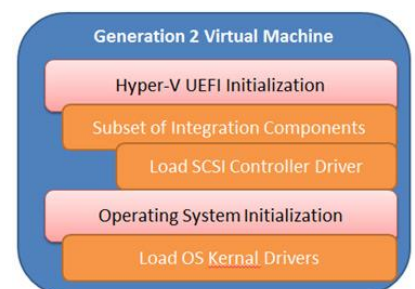
FIGUR 5

Billede:

<http://www.slideshare.net/rsnarayanan/security-best-practices-for-hyper-v-and-server-virtualization>



FIGUR 7



FIGUR 6

<sup>16</sup> [https://msdn.microsoft.com/en-us/library/cc768520\(v=bts.10\).aspx](https://msdn.microsoft.com/en-us/library/cc768520(v=bts.10).aspx) (15-05-2015)

<sup>17</sup> <http://www.serverwatch.com/server-tutorials/hyper-v-2012-r2-pros-and-cons-of-generation-1-vs.-generation-2-vms.html> (18-05-2016)

### 7.3 Middleware<sup>18</sup>

Middleware er en fælles betegnelse for en applikation eller protokoller der gør det muligt at 2 separate systemer kan kommunikere sammen. For at en applikation eller protokol kan betegnes som middleware skal det tilbyde et API (application programming interface). F. eks er TCP, vSwitchs, NAT middleware.

### 7.4 Protokoller

Vi vil dette afsnit forklare teoretisk, hvordan TCP, NTP og UDP protokollerne fungerer, som giver en bedre forståelse for, hvordan vi kan forbedre sikkerheden senere i rapporten.

#### 7.4.1 Network Time Protocol (NTP)<sup>19</sup>

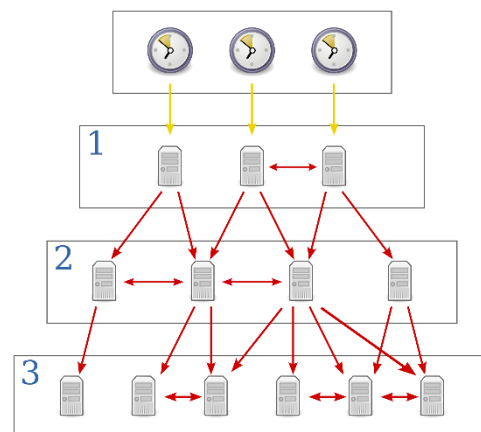
NTP er en internet protokol der bruges til clock synchronization mellem computers, protokollen kører efter Coordinated Universal Time (UTC) tid og er designet til at sørge for at de computer der snakker sammen kører efter denne tid som ses i Figur 8.

Denne protokol er som regel brugt i et client-server system. Det kan også bruges i peer-to-peer systemer hvor begge peers ser modparten som en potentiel tids kilde.

#### 7.4.2 User Datagram Protocol (UDP)<sup>20</sup>

UDP er endnu en af kerne protokollerne i "internet protocol suite" men til forskel fra TCP er UDP protokollen connectionless baseret, hvilket betyder at der ikke er nogen kontrol på om en pakke, når frem til modtager. Dette gør at protokollen er hurtigere. De pakker der bliver sendt er mindre, UDP bruges som oftest til kommunikation, hvor hastighed er vigtigere end at alle pakker når frem, som eksemplet video strømming,

UDP's header er også betydelig mindre og består kun af 4 felter, som er følgende.



FIGUR 8

Billede:

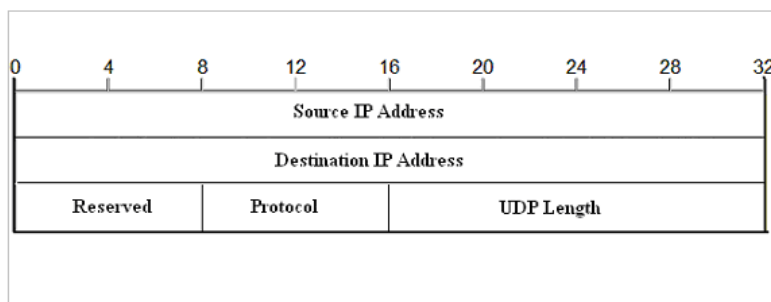
[https://en.wikipedia.org/wiki/Network\\_Time\\_Protocol](https://en.wikipedia.org/wiki/Network_Time_Protocol)

#### 4 felter

- Source port number
- Destination port number
- Length
- Checksum

*Note: Checksum feltet er ved brug af IPV4 valgfrit, men påkrævet ved brug af IPV6.*

#### UDP header illustration



FIGUR 9

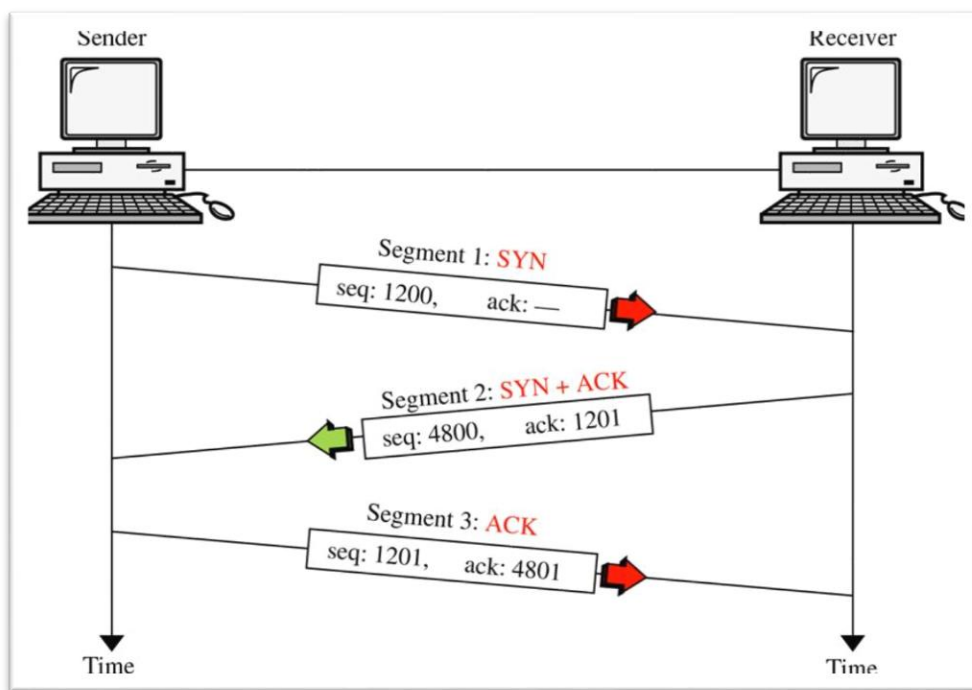
<sup>18</sup> [1, side 687, Middleware]

<sup>19</sup> [https://en.wikipedia.org/wiki/Network\\_Time\\_Protocol](https://en.wikipedia.org/wiki/Network_Time_Protocol) 10/5-2016

<sup>20</sup> [https://en.wikipedia.org/wiki/User\\_Datagram\\_Protocol](https://en.wikipedia.org/wiki/User_Datagram_Protocol) 10/5-2016

### 7.4.3 Transmission Control Protocol (TCP) <sup>21</sup>

TCP er en af kerne protokollerne i "internet protocol suite" og er en connection baseret protokol, hvilket betyder at der skabes en stabil forbindelse mellem de to maskiner der skal kommunikere. TCP bruges derfor til kommunikation, hvor det er vigtigere at pakkerne, når frem end at det går hurtigt. Forbindelsen oprettes ved hjælp af "3 way hand shake" som vist på billedet her under



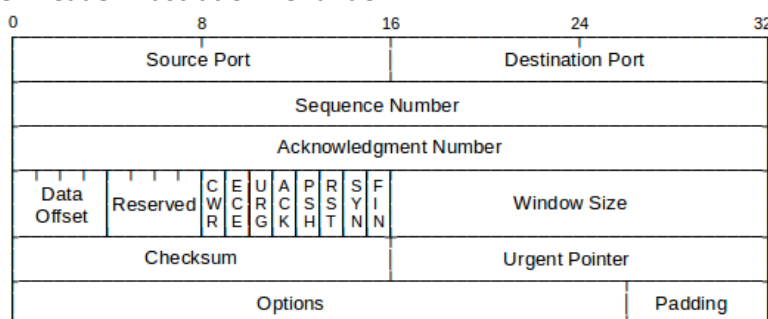
FIGUR 10

TCP sender data i form af pakker kaldet "Segments", hver data pakke (segment) består af en Header del og en data del. Header delen består af 10 obligatoriske felter.

#### 10 obligatoriske felter

- Source port (16 bits)
- Destination port (16 bits)
- Sequence number (32 bits)
- Acknowledgment number (32 bits)
- Data offset (4 bits)
- Reserved (3 bits)
- Flags (9 bits) (aka Control bits)
- Window size (16 bits)
- Checksum (16 bits)
- Urgent pointer (16 bits)

TCP header illustration her under.



FIGUR 11

<sup>21</sup> [https://en.wikipedia.org/wiki/Transmission\\_Control\\_Protocol](https://en.wikipedia.org/wiki/Transmission_Control_Protocol) 10/5-2016

## 8 Udvikling af prototyper

I dette afsnit vil vi forklare praktisk, hvordan vi har fuldført prototyperne med basale krav, implementering og validering. Vi har brugt prototyperne's validering til følgende:

- Analysere, hvilke prototyper vi kan bruge til at forfine kravspecifikationen
- Analysere, hvilke fordele og ulemper der er i softwaren for prototyperne

Disse prototyper har vi delvis også brugt i final implementering.

### 8.1 Basal kravspecifikation

Kravene for prototyperne kan findes i [Kravspecifikation under Prototyper](#).

### 8.2 Implementering

Vi har i dette afsnit taget udgangspunkt i kravspecifikationen, og derefter gået direkte til implementering. Vi læste på teorien undervejs for softwaren.

Prototype	Beskrivelse af forsøgsimplicering
<b>Hardware prototype test</b>	<p>Vi startede ud med at bruge en lille computer med en dual-core processor, 4 GB og 200 GB SATA harddisk, fordi det ud fra vores teori afsnit <a href="#">hardware requirements for Windows Server 2012 R2</a> at det var en god ide.</p> <p>Vi installerede Windows Server 2012 R2 operativ system og installerede rolen Hyper-V og hostede 3 virtuelle servere med samme operativ system. Efterfølgende installerede vi features i de virtuelle server med Windows Server 2012 R2, som kan ses herunder.</p> <p><b>Virtuel server 1 – Active directory – Domain controller</b> Vi installerede Active directory og joined alle virtuelle maskiner til følgende domain controller, samt satte kontoer, grupper, brugerrettigheder og justerede i konfigurationer.</p> <p><b>Virtuel server 2 – Web server</b> Vi installerede rollen IIS med alle features (F. eks ASP.NET) og prøvede at tilgå den ude fra.</p> <p><b>Virtuel server 2 – database server</b> Vi installerede Microsoft SQL Server 2015 og management clienten og prøvede at tilgå den ude fra og på domain netværket.</p> <p>Efterfølgende fik vi fat i en stærkere Blade maskine med 12 kerne processor, 42 GB og en hurtigere 300 GB harddisk, hvor vi fik hjælp til at installere ESXI operativ system af Ib fra UCN.</p> <p>Vi havde ikke selv fysiks adgang til serveren på skolen, fordi den var vedligeholdt af Ib fra UCN.</p>
<b>Windows Server 2012 R2</b> Basis features	<p>Vi fik mere viden om software arkitekturen bag Microsoft produkter ved følgende:</p> <ul style="list-style-type: none"><li>- Installer og konfigurer Windows Firewall, Hyper-v, Windows Backup, Active directory og Powershell.</li><li>- Skifte imellem Server-core og GUI-interface i tilfælde af performance forbedring.</li><li>- At skrive Powershell scripting til at backup Hyper-v virtuelle maskiner</li></ul>



	<ul style="list-style-type: none"> <li>- Windows Server automatisk licens aktivering</li> </ul>
<b>ESXI Server</b> Opsætning af en virtuel server	<p>På Blade maskinen via remote opsatte vi ressource pools til at adskille ressourcer af CPU kraft og RAM i grupper. Vi tilføjede derefter en virtuel server til en ressource pool.</p> <p>Efterfølgende tilføjede vi et virtuel netværk og harddisk til den virtuelle server.</p> <p>Vi installere Windows Server 2012 R2 på den virtuelle server og prøvede at installere Hyper-v rollen, men det var ikke muligt</p>
<b>Windows Server 2016 technical preview</b> Guest hyper-v host	<p>Vi installerede Windows Server 2016 technical preview som virtuel server på ESXI serveren, for at finde ud af om vi kunne bruge den som virtuel hypervisor til at installere nested virtuel maskiner med Hyper-v.</p>
<b>ESXI server og konfiguration</b>	<p>Vi brugte ESXI til at lave en virtuel hypervisor med Windows Server 2012 R2 i stedet for Windows Server 2016 technical preview.</p> <p>Vi prøvede, ved at lave en speciel konfiguration som ESXI understøttede, men det er ikke officielt supportet af VMWare.</p> <p>Vi ændrede følgende indstillinger i vmx filen, som bruges af ESXI serveren til at indlæse indstillinger til en virtuel server. Så blev det muligt at få Windows Server 2012 R2 til at bypass tjek om den kører i et virtuelt miljø. Vi testede både netværk og performance på nested virtuelle maskiner.</p> <ul style="list-style-type: none"> <li>- mce.enable = "TRUE"</li> <li>- hv.enable = "TRUE"</li> <li>- hypervisor.cpuid.v0 = "FALSE"</li> </ul> <p><b>Guide fra internettet vi brugte</b>  <a href="https://communities.vmware.com/docs/DOC-8970">https://communities.vmware.com/docs/DOC-8970</a>  <a href="https://communities.vmware.com/thread/520147?start=0&amp;tstart=0">https://communities.vmware.com/thread/520147?start=0&amp;tstart=0</a></p>
<b>Windows Server 2012 R2</b> Routing, NAT, DNS og DHCP	<p>Vi installerede alle NAT, DNS og DHCP features på virtuel maskine på vores ESXI Server med operativ system Windows Server 2012 R2.</p> <p>Vi lavede konfiguration for DHCP, så den kunne uddele IP adresser over LAN med følgende ranges 192.168.137.2-192.168.137.255 og med 192.168.137.1 som router IP.</p> <p>Derudover konfigurere vi DNS, så at IP-adressen 192.168.137.1 også kunne bruges til DNS server.</p> <p>NAT bevarede vi default indstillinger som Microsoft havde sat og internettet med TCP/UDP protokollerne virkede derefter på alle virtuelle maskiner på samme netværks adapter som denne maskine havde.</p> <p>Vi installerede også en VPN feature og oprettede en konto for sig til følgende med begrænset bruger rettigheder og policy for kontoen, for hvor mange gange man må indtaste forkert password før låsning af konto.</p>
<b>Kali linux</b> Basis features	<p>Vi installerede Kali linux v2 i en virtuel nested maskine og tjekkede følgende:</p> <ul style="list-style-type: none"> <li>- At scanning tools virkede</li> <li>- At der var internet</li> </ul>
<b>ESXI server</b> VLAN	<p>Vi testede om datapakker var adskilt, når man gav VLAN ID's til de forskellige virtuelle switches på ESXI serveren. Vi brugte Kali linux v2 tools til at opsnappe trafikken.</p> <p>Vi afprøvede "uheldigt" også, hvad VLAN 0 var til, hvilket vi kommer nærmere ind på under testen.</p>

<b>IDS</b> OSSEC system	Vi installerede IDS packet systemet OSSEC i et CentOS linux operativ system på en nested virtuel server. Vi testede om det var muligt at få adgang til logfiler med advarsler og om der var internet derpå.
----------------------------	---

### 8.3 Validering af krav

Vi vil i dette afsnit beskrive, hvilke ting der lykkes under implementering af prototyperne og hvilke ting der lever op til basis kravspecifikationen.

Prototype	Test validering
<b>Hardware prototype test</b>	<p>Både vores lille server og Blade server understøttede begge Windows Server 2012 R2 og ESXI.</p> <p>Vi fandt hurtigt ud af, at hvis du har mere end 2 virtuelle servere skal du have en processor med flere end 4 kerner, samt over 10 GB RAM og 200 GB harddisk plads.</p> <p>Virtualisering kræver mange ressourcer, hvilket vi også havde regnet med, da vi kiggede på Windows Performance Monitor i Windows operativ systemet.</p> <p>Blade serveren fra UCN skolen gjorde det nemmere og hurtigere at implementere virtuelle maskiner. Alt på maskinen gik hurtigere.</p> <p>Vi var forhindret til at få adgang til Blade serveren fysisk uden Ib's tilstedeværelse fra UCN, hvis der opstod remote adgang problemer.</p> <p>Det var et krav fra UCN, for at kunne bruge Blade serveren. Det var heller ikke et krav fra os, at få fysisk adgang, fordi vi ikke vil stå for hardware vedligeholdelse.</p>
<b>Windows Server 2012 R2</b> Basis features	<p>Med Windows Server 2012 R2 blev vi overrasket over, hvor utrolig nem det er at sætte op, fordi at der er god dokumentation fra Microsoft til deres features i operative systemet.</p> <p>Active directory hjælper med brugerstyring, administration og software licens aktivering.</p>
<b>ESXI Server</b> Opsætning af en virtuel server	<p>Vi kunne tydelig mærke i praktisk at VMWare's <a href="#">vSphere client software beskrevet i teorien</a> er brugervenlig og nem at arbejde med, når du skal administrere og konfigurere virtualisering.</p> <p>De bruger ufattelig mange begreber, hvilket kræver meget oplæring.</p> <p>Vi fandt også ud af, at det var muligt at tilføje og fjerne ressourcer som f. eks harddiske og netværks adapter uden at skulle slukke virtuelle servere.</p> <p>Hvorimod virtuelle kerner og RAM kunne du kun prioritere efter procent, hvem som skulle have mest adgang efter tid. Det var ikke muligt at tilføje nye virtuelle kerner eller RAM uden at genstarte maskinen.</p>
<b>Windows Server 2016 technical preview</b> Guest hyper-v host	<p>Vi fandt ud af, at Microsoft ikke var klar eller understøttede nested virtuel server i deres beta versioner af Windows Server 2016 endnu, men det kommer snart siger de.</p> <p>Vi fik blot følgende fejlmeddelelse ved forsøg på at installere Hyper-v featuren på en virtuel server på ESXI'en "<b>Hyper-v cannot be installed. A hypervisor is already running</b>".</p>
<b>ESXI server og konfiguration</b>	<p>Ved at bruge disse indstillinger var det muligt at lave virtuel hypervisor med Windows Server 2012 R2 som indeholdte nested virtuel server med Windows Server 2012 R2.</p> <p>Vi fik problemer med internettet ikke virkede på nested virtuelle servere. Det var, fordi MAC-adresserne ikke kunne registreres</p>



	<p>automatisk i ESXI hypervisoren, så vi måtte slå Promiscuous Mode til for den virtuelle hypervisor med Windows Server 2012 R2.</p>
<p><b>Windows Server 2012 R2</b> Routing, NAT, DNS og DHCP</p>	<p>Vi fik den overraskelse at man sagtens kan bruge Windows Server 2012 R2 som en router, fordi vi fandt ud af, at den indeholder alle de features der er nødvendig for os i en virtuel infrastruktur.</p>
<p><b>Kali linux</b> Basis features</p>	<p>Vi fandt ud af at Kali Linux v2 er det rigtig godt gratis værktøj nogensinde til at lave penetration testing. Der er rigtig god dokumentation til operativ systemet. Det kan teste og indsamle informationer om mulige svagheder indenfor kort tid for både hjemmesider, software, server infrastruktur, netværk, WIFI og mere. Det har ufattelig mange tools og du kan være klar til at teste på under en halvtime. Det er brugervenligt, til en professionel systemadministrator og udvikler.</p> <p>Du kan også bruges til at lave et angreb, men det kræver mere manuelt arbejde.</p>
<p><b>ESXI server</b> VLAN</p>	<p>Vi fandt ud af, at adskille netværk på en ESXI server var nemt med VLAN ID's på vSwitchs, dog erfarede vi, at vi aldrig skal ændre VLAN ID 0 på den eksterne fysiske hovedlinje ved en fejl. Vi mistede internet forbindelsen til ESXI serveren. Så vi læste videre på teorien omkring VLAN 0 og ESXI serveren, hvilken betydning den har.</p> <p>Vi kom til at den eneste måde ESXI serveren ved at datapakker skal ud på den eksterne linje er den tydeligt ved, hvilken vSwitchs der er den eksterne linje og hvilken en der er til de virtuelle servere.</p>
<p><b>IDS</b> OSSEC system</p>	<p>Vi fandt ud af, at det ufatteligt svært at sætte IDS op, men det er godt værktøj til at få hurtig overblik af log filer med oplysninger om angreb i ens netværk, operativ systemer og andre applikationer, samt der mange integrationer til følgende.</p>

## 9 Forfin kravspecifikation

Du kan i dette afsnit læse dele af de eksisterende krav fra afsnittet [Basal kravspecifikation](#), som vi har forfinet efter implementering og validering af prototyperne.

### 9.1 Funktionelle krav

Vi har forfinet listen med på eksisterende og nye tilføjede krav således.

#### 9.1.1 Systemadministrator

Som systemadministrator er det vigtig at kunne overvåge og få adgang til logfiler hurtigt og nemt, samt at administrerer og konfigurer via en remote adgang.

##### 9.1.2.1 Features

- Remote adgang via internet forbindelse
- Tilføj, konfigurer og slet virtuel server
- Tilføj, konfigurer og slet virtuel netværk
- Tilføj, konfigurer og slet virtual harddisk
- Tilføj, konfigurer og slet brugerrettigheder og system kontoer for egne interne systemer.
- Tilføj, konfigurer og slet service adgang.
- Installere og konfigurer egne applikationer
- Send og modtag e-mail
- Adgang til alle logfiler fra en maskine
- Ressourcestyring
- Remote installation af et operativt system for en virtuel maskine
- Remote styring af alle maskiner fra en virtuel maskine.
- Styring og konfigurer overvågningsværktøj (IDS)
- Læse og besvar support tickets

#### 9.1.2 Kunde

Som kunde er det vigtigt at kunne skalere ressourcer, installere egne applikationer på en virtuel maskine og have remote adgang. Vi er kommet frem til følgende features vi ønsker til en kunde.

##### 9.1.2.2 Features

- Remote adgang via internettet
- Skalere garanteret ressourcer
- Installere og konfigurer egne applikationer på abonnementsbaseret virtuelle servere
- Læse og skrive til en eller flere ekstern virtuel backup over netværk
- Adgang til kontrolpanel til konfiguration af tilknyttet virtuelle maskiner
- Tilføj support ticket til systemadministrator
- Se egne support ticket og deres status
- Mulighed for eksport af virtuel server

## 9.2 Ikke funktionelle krav

Vi har forfinet listen med på eksisterende og nye tilføjede krav således.

### 9.2.1 Systemadministrator og udvikler

Det er vigtigt at, så meget som mulig er automatiseret, sikkert og performer godt, samt at systemadministrator ikke afhængige af bestemt en softwareleverandør.

#### 9.2.2.1 Sikkerhed, backup og overvågning

- Kryptering af datatrafik ved remote adgang
- Automatisk midlertidig lukning af remote adgang i tilfælde af password brute force
- Filtrering og blokering af services og porte
- Automatisk overvågning og gem af alle logfiler med automatiske rates af advarsler for angreb
- Automatisk beskyttelse mod DDOS angreb
- Automatisk backup af interne systemer og kunder

#### 9.2.2.2 Platformkrav

- Support for Linux & Windows Server 2008/2012/2012 R2

#### 9.2.2.3 Performance

- Automatisk skalere af ressourceforbrug for CPU, internetforbindelse og RAM imellem interne systemer

#### 9.2.2.4 Integrationskrav

- Automatisk licens aktivering for Windows Server maskiner
- Mulighed for at integrere egne systemer

### 9.2.2 Kunde

Det er vigtig for kunden at transparencies er vægtet højt, så de kan have fokus på deres forretning og udvikling og mindre vedligeholdelse af hardware.

#### 9.2.2.5 Sikkerhed, backup og overvågning

- Mulighed for kryptering af datatrafik ved remote adgang
- Automatisk backup af systemer og kunders virtuelle servere
- Automatisk mindsker DDOS angreb
- Isolering af operativ system
- Isolering af intern netværk

#### 9.2.2.6 Platformkrav

- Support for Linux og Windows Server 2008/2012/2012 R2

#### 9.2.2.7 Performance og elasticity

- Automatisk skalere shared ressourceforbrug for CPU, internetforbindelse og RAM
- Automatisk garantere ressourceforbrug
- Hver virtuel maskine skal kunne have en response tid under 100 latency på et netværk.

#### 9.2.2.8 Integrationskrav

- Automatisk licens aktivering for kunders Windows Server maskiner

## 9.3 Hardware

Vi har forfinet listen med på eksisterende og nye tilføjede krav således.

- Det er et krav for os, at undgå hardware vedligeholdelse, fordi dele eller alt infrastruktur skal være fleksible at flytte til forskellige datacentre over en internet forbindelse på kort tid, derfor ønsker vi et virtuel infrastruktur på et fysisk infrastruktur vedligeholde af et datacenter.
- Mulighed for hot plug feature i bundkort hardwaren, men er ikke et "must have"
- Billig CPU, RAM og harddisk hardware, langsigtet.
- Hver maskine skal kunne have en response tid på under 110 latency på et netværk i samme land.

## 10 Analyse

Vi vil i dette afsnit analysere, hvilke trusler som oftest forekommer for virksomheder. Dette kan hjælpe os med at træffe bedre designvalg til at beskytte vores system mod oftest forekommende trusler.

### 10.1 <sup>22</sup>Analyse af IT trusler mod virksomheder

Ved et datacenter, involvere det en enorm mængde data, og som følge af det, er datacentrene også mere udsat for angreb. De er stort set konstant udsat for at blive scannet og analyseret for sårbarheder med diverse tools, samt social Engineering som har til formål at skaffe så mange informationer omkring en virksomhed eller et datacenter som muligt. Disse angreb er, af mange forskellige typer, men den hyppigste type angreb er DDoS. Formålet med at angribe et datacenter, er som oftest ikke datacenteret i sig selv, men centerets kunder i form af virksomheder.

Baggrunden for disse angreb er forskellige, alt fra økonomiske formål, til politiske begrundelser, for at skaffe følsom eller fortrolige oplysninger, der kan bruges til afpresning eller videresælges.

#### 10.1.1 Generel trusselsvurdering for virksomheder og staten, fra Center for Cybersikkerhed<sup>23</sup>

Denne tabel herunder er taget udgangspunkt i rapportererne fra Center for cybersikkerhed og Symantec fra 2015.

Trussel	Niveau
Cyberspionage	Meget høj
Cyberkriminalitet	Meget høj
Cyberaktivist	Middel
Cyberterror	Lav

#### 10.1.2 Typer af angreb

[www.infosecurity-magazine.com](http://www.infosecurity-magazine.com) skriver at de 5 oftest brugte angreb er

- DDoS Attacks
- Web Application Attacks
- DNS Infrastructure Exploits
- SSL-Induced Security Blind Spots
- Weak Authentication and Brute Force Attacks

### 10.2 Konklusion af analyse

Vi har fået opfattelsen at overvågning og cyberkriminalitet er næsten umuligt at beskytte sig imod, fordi det oftest handler om hvor mange computer ressourcer angriberen (blackhatten) har. Det handler mere eller mindre om, hvor lang tid du kan holde dem ude efter behov. Det er vanskeligt at blokere dem 100%.

F. eks er scanning af netværk vanskeligt at beskytte sig imod.

---

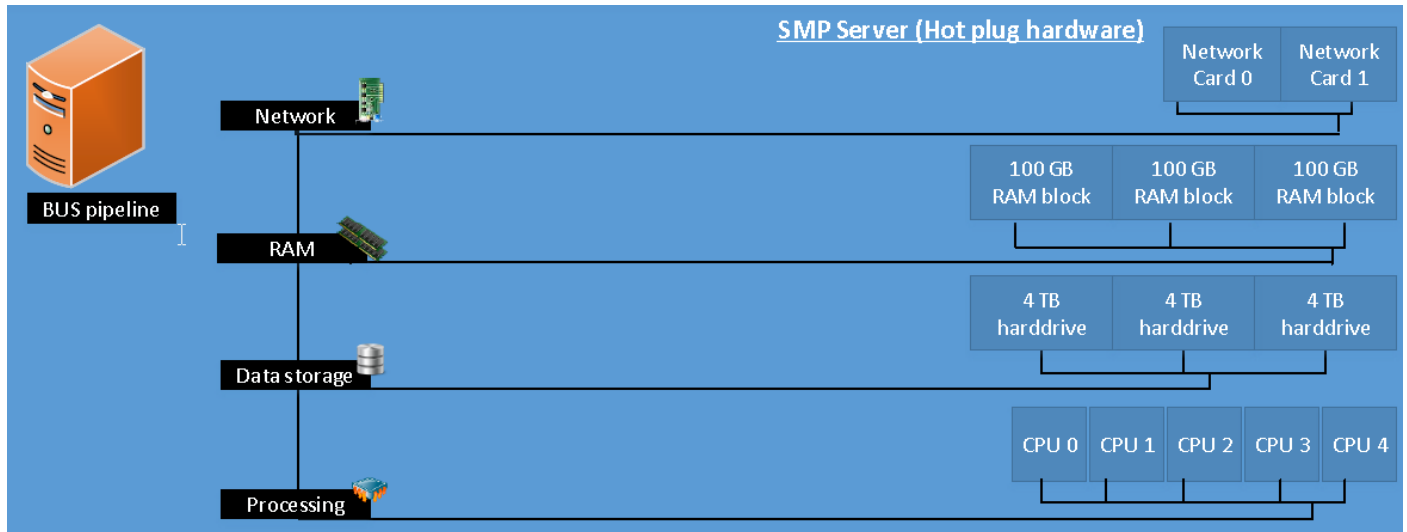
<sup>22</sup> [http://www.symantec.com/security\\_response/publications/monthlythreatreport.jsp](http://www.symantec.com/security_response/publications/monthlythreatreport.jsp) (17/3-2016)

<sup>23</sup> <https://fe-ddis.dk/cfcs/CFCSDocuments/Cybertruslen%20mod%20Danmark%202016.pdf> (17/3-2016)

## 11 Design

Formålet med designet er, at opnå systemet skal være sikkert og nemt at vedligeholde og administrere. Vi har derfor valgt at lave et system, der kører meget automatiseret, når det er i produktion.

### 11.1 Hardware infrastruktur



Vi har valgt at genbruge hardware til vores system som ses på billedet oven over, fordi det er billigere, skåner vores miljø, da genbrug af hardware betyder mindre affald. Ulempen er en større risiko for hardware bliver defekt og skal udskiftes.

Vi har valgt den dyre løsning i form af hot plugging / hot swapping (lidt i retning af mainframes). Vi undgår på den måde at skulle slukke for systemet, ved tilføjelser af nye ressourcer, som sikre en høj oppe tid.

Ud fra vores krav om at vi ikke vil håndtere hardwaren, har vi valgt at outsource på dette område.

#### Fordele

- Mindre udgifter til fysisk overvågning, tyveri og beskyttelse af hardware
- Mindre behov for udskiftning af brudt hardware med integreret krypteringsalgoritme
- Høj availability
- Billigere på langsiget
- Mindre krav for hardware uddannelse og kurser
- Miljø venligt
  - Mindre affald
  - Mulighed for tilskud til staten
  - Højere markedsføringsværdi, flere kunder

#### Ulemper

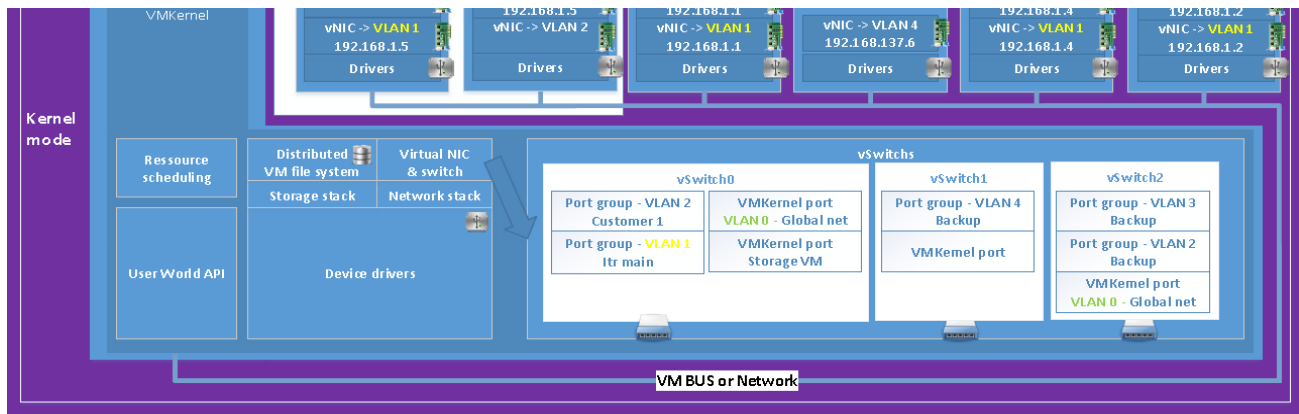
- Mangel på fysisk kontrol af hardware ved mistillid af leverandør
- Deling af internet forbindelse med andre virksomheder med høj datatrafik.
- Større risiko for data tab eller brud på forbindelsen ved angreb på andre virksomheder på samme hoved forbindelse
- Hardwaren er dyr ved opstart
- Større risiko for single point of failure på bundkort

## 11.2 Virtuel infrastruktur i ESXI Server og arkitektur

Vi har valgt at bruge ESXI til vore virtuelle infrastruktur, fordi at denne kernel software understøtter nede virtualisering. Vi har valgt at holde vores virtuelle infrastruktur adskilt fra de kunde baseret virtuelle infrastruktur, blandt andet grundet sikkerhed. Vi bruger virtuel Lan(VlanID<sup>24</sup>) til yderligt at holde visse servers i vores infrastruktur adskilt fra hinanden, da VlanID svare til en fysisk adskillelse af de virtuelle switches(vSwitches). Vi har også valgt at adgang til ESXI'en kun kan opnås via USB nøgle eller VPN.

### 11.2.1 Virtuel netværk

Du kan herunder se dele af et diagrammet, der viser netværk og vSwitchs til de forskellige virtuelle servere. Du kan se hele diagrammet i [Bilag 2](#).



#### 11.2.1.1 vSwitches

Vi har valgt at adskille vores netværk med 3 vSwitches

##### VLAN

Vi har valgt at bruge Vlans til yderligt at adskille netværket for vores virtuelle infrastruktur. Hver Vlan har et ID som bliver sat på data pakker som et tag med ID'et så systemet ved hvor pakken skal hen og for hvilke enheder der har tilladelse til at se dem.

VlanID 0 er default<sup>25</sup> konfigureret til at være det ID der bruges til eksternt kommunikation.

##### VM Kernel

Vi har valgt at bruge VMkernel i vSwitch0, for at kunne remote til ESXI serveren i host management med vSphere client, samt vi bruger iscsi som gør det muligt at tilføje virtuel storage til at host virtuelle maskiner i. Der er mulighed for ESXI monitoring tools til overvågning af ressourcebrug og netværkstrafik.

- **vSwitch0** er til vores interne netværk
- **vSwitch1** er uden adgang til internettet for at mindske belastningen af trafik og uautoriseret adgang.
- **vSwitch2** er til kundernes vm's, for at beskytte vores infrastruktur mod belastning af data trafik til og fra kundernes vm's.

##### Fordele

- Bedre load balance af netværk, derved mindre belastning ved DDOS angreb
- Sikre hurtigere backup af kundernes og vores egne VM's
- Mere kontrol og mulighed for overvågning
- Mindsker risiko for uautoriseret adgang

##### Ulemper

- Mere vedligeholdelse
- Mere komplekst og kræver mere faglig viden

<sup>24</sup> <https://pubs.vmware.com/vsphere-51/index.jsp?topic=%2Fcom.vmware.vsphere.networking.doc%2FGUID-7225A28C-DAAB-4E90-AE8C-795A755FBE27.html> 26/5-2016

<sup>25</sup> [https://kb.vmware.com/selfservice/microsites/search.do?language=en\\_US&cmd=displayKC&externalId=1004074](https://kb.vmware.com/selfservice/microsites/search.do?language=en_US&cmd=displayKC&externalId=1004074) 1/6-2016

### 11.2.1.2 Load Balance

Vi har valgt at bruge vSwitches til at lave load for vores og kunderne virtuelle infrastruktur, i et forsøg på at mindske risikoen for databas eller belastning under eventuelle DDoS angreb.

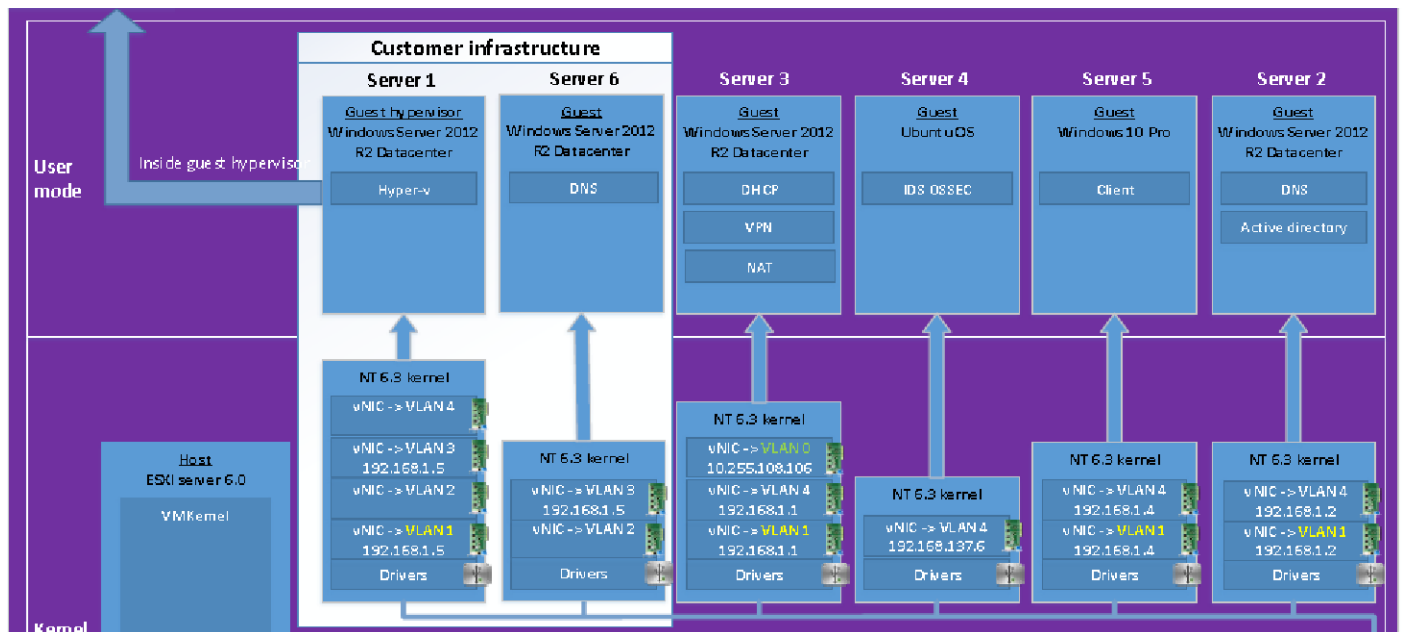
#### Fordele

- Mulighed for sortering af pakker
- Reducer belastning af data trafik forbindelse
- Mindsker risiko for nedetid
- Mulighed for caching af data request, derved giver højere performance

#### Ulemper

- Forøger latency af data pakker
- Mere vedligeholdelse

### 11.2.2 Virtuelle servers



Vi har valgt at hver af vores virtuelle server har en firewall. Du kan se alle virtuelle server på billedet oven over.

#### 11.2.2.1 Server 2

Vi har valgt at oprette en Active directory domæne controller med intern DNS, som vi bruger til at administrere bruger rettigheder, DNS, software licens, driftovervågning, push af patches og systemindstillinger på en eller flere maskiner.

#### Fordele

- Mulighed for høj krypteret trafik mellem maskinerne på domænet
- Låsning af en eller flere computers brugere/kontoer ved brug af force password angreb
- Administrator konto har adgang til alle maskiner på domænet.
- Fælles bruger/konto database

#### Ulemper

- Single point of failure
- Flexible remote adgang ved fejl konfiguration af brugerrettigheder/computerrettigheder
- Større risiko for databas ved uautoriseret adgang til admin konto.

### 11.2.2.2 Server 3

Vi har valgt at kombinere DHCP, NAT og VPN på samme server for at spare ressourcer.

#### 11.2.2.2.1 DHCP

Vi har valgt at bruge DHCP server til at administrere og tildele IP adresser, til at gøre det nemmere at identificere enheder/gæster i vores interne netværk.

##### Fordele

- Automatisering af netværk administration
- Mindre behov for IPv4 public adresser
- Sikre vedvarende statisk IP, ved genstart eller flytning af intern virtuel infrastruktur

##### Ulemper

- Komplet konfiguration ved større netværk
- Svaghed ved IP scanning af host's
- Single pointer failure

#### 11.2.2.2.2 NAT

Vi bruger NAT til at oversætte vores private IP's til vores public IP.

##### Fordele

- Deling af public IP til private IP's.
- Mulighed for anonymitet
- Mindsker behovet for public IPv4 adresser.

##### Ulemper

- Risiko for forsinkelse af data pakker
- Single pointer failure
- Anonymitet for eksterne brugere

#### 11.2.2.2.3 VPN

Vi har valgt at bruge VPN til at lave remote forbindelse til vores infrastruktur med ekstra beskyttelses lag/dør til vores interne netværk.

##### Fordele

- Høj kryptering ved remote forbindelse
- Lock out ved gentagelse af uautoriseret adgang
- Ekstra lag/dør for adgang

##### Ulemper

- Sænker forbindelsen
- Ved for 3 forkerte password indtast låses bruger konto i 24 timer. Nødvendig for fysisk adgang.

## 12 Server 4

Vi har valgt at bruge trejdepart software IDS til at overvåge netværk, file manipulation, brugerrettigheder og generelt angreb for at vi system administratorer kan forhindre skade på systemet eller uautoriseret adgang.

##### Fordele

- Hjælper med at få overblik af forsøg på angreb, manipulation og uautoriseret adgang.
- Virus tracking

##### Ulemper

- Øger belastning på netværk og hardware ressourcer
- Meget komplet opsætning og behov for højt faglige medarbejdere
- Vedligeholdelse er høj
- Risiko for falske alarmer



## 13 Server 5

Vi har valgt at adgangen til infrastrukturen opnås via en virtuel klient desktop som kun kan opnås adgang til via VPN. Den virtuelle klient giver så adgang til remote desktop til de andre maskiner, dog begrænses de evt. ansattes adgang til hoved systemet.

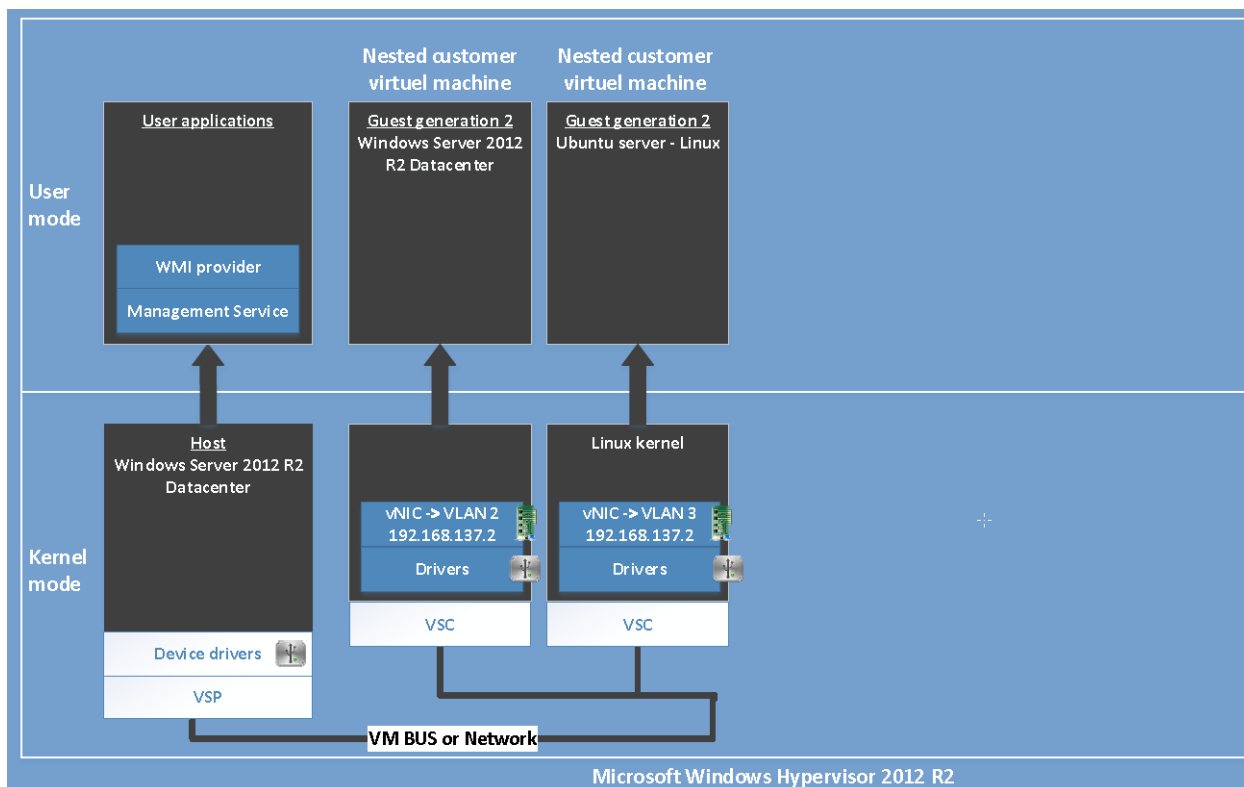
### Fordele

- Mere kontrol af medarbejder adgang
- Mindre risiko for ekstern uautoriseret
- Flere lag/døre ind til interne servere
- Remote desktop arbejdsplads
- Mindre overvågning af remote adgang

### Ulemper

- Flere sårbarheder i GUI
- Større risiko for medarbejder fejl

### 13.1.1.1 Server 1



Vi har valgt at lave en virtuel hypervisor som ses på billedet oven over, fordi det giver mulighed for at lave test/development miljø ved opgradering af operativ system uden nedetid. Vi har valgt Windows Server 2012 R2 datacenter som hypervisor OS på grund af ubegrænset licens til virtuel Windows Server 2012 R2 datacenter fra Microsoft, og automatisk aktivering af licenser.

### Fordele

- Mulighed for mere kontrol, overvågning og administration af hypervisor med Active Directory
- Mulighed for test/development miljø
- Mindsker behovet for at købe hardware ved opgradering af hypervisor OS.
- Mindre behov for antallet af bundkort
- Linux support i Windows Server 2012 R2 hypervisoren

### Ulemper

- Risiko for dårlig performance
- Meget komplekst og dyrt
- Risiko for virtuel infrastruktur kollaps ved defekt bundkort

- Mulighed for salg af hypervisor til større virksomheder med større tekniske krav.

## 13.2 Virtuel harddisk og backup

Vi har valgt at virtuelle harddiske placeres på fysiske harddiske på samme dedikeret maskine.

For hver 2 fysiske harddiske har vi kun en harddisk på grund af raid 1 på hardware niveau.

Hver harddisk er SSD for at øge performance. Antallet af harddiske er efter behov i forhold til kundernes krav.

De virtuelle harddiske som indeholder OS's placeres ikke på samme fysiske som virtuelle backup harddiske for at undgå data tab ved defekt harddiske.

Backup er automatiseret af Windows Server Backup feature.

### Fordele

- Performance øges
- Mindsker risiko for datatab
- Der er mulighed for kryptering af data

### Ulemper

- Ved fysisk skade er der større risiko for datatab

## 14 Final Implementering

Vi vil i dette afsnit forklare, hvilke udfordringer og problemer vi har haft under implementeringsforløbet.

### 14.1 Valg af hardware

Vi startede med at implementere del af systemet med prototyper på gammelt hjemme hardware med en dual-core processor, 4 GB ram og 200 GB harddisk. Vi fik hurtigt opfattelse af, at de ressourcer ikke kun leve op til vores krav til performance, derefter opsøgte vi hjælp af UCN til at få adgang til IT LAB igennem Ib og Per for at få adgang til flere hardware ressourcer.

De første 4 dedikerede maskiner vi prøvede på UCN understøttede ikke Windows Server 2012 R2, samt vi var meget i tvivl, hvor meget af infrastrukturen kunne være virtuelt.

Vi diskuterede om det var nødvendigt at have active directory på sin egen maskine for at joine en hypervisor til et domæne end til vi kom i tanken om en virtuel hypervisor.

Efterfølgende skiftede vi til en Blade server som vi fik rådighed til af UCN med 12 kerne processor, 42 GB og 300 GB harddiske og 300 GB netværksharddisk, som vi tydeligt kunne mærke øgede performance gevaldigt.

### 14.2 Servere & Clients

Vi har installeret følgende servere og klienter herunder

#### 14.2.1 ESXI hypervisor

ESXI hypervisoren er installeret som det første OS led med følgende virtuelle servere.

Server	Operativ system	Beskrivelse
Server 1	Windows Server 2012 R2 Datacenter Hypervisor	Hypervisor maskine med nested virtuelle maskiner.
Server 2	Windows Server 2012 R2 Datacenter	DNS og Active directory
Server 3	Windows Server 2012 R2 Datacenter	DHCP, VPN og NAT
Server 4	Windows Server 2012 R2 (Skulle have været Ubuntu)	Denne maskine var oprindelig en proxy server, men vi fandt ud af det ikke var nødvendigt, fordi vswitchs i ESXI har features til load balance til at kunne beskytte mod DDOS og belastning på netværk. Vi skulle have skiftet denne ud med en IDS med OSSEC..
Server 5	Windows 10 Pro	Remote klient til at remote alle servere intern
Server 6	Windows Server 2012 R2 Datacenter	DNS til kunderne

#### 14.2.2 Virtuel Windows Server 2012 R2 hypervisor

Windows Server 2012 R2 hypervisor er installeret som en virtuel maskine med følgende nested virtuelle maskiner.

Server	Operativ system	Beskrivelse
Kunde server 1	Windows Server 2012 R2 Datacenter	Testet nested kunde server
Penetration test client machine	Kali linux v2	Maskine vi har brugt en masse tools til at teste
IDS OSSEC server	Ubuntu (Skulle slettes)	Denne maskine skulle flyttes til ESXI hypervisoren, men på grund af reserveret dataplads manglen placerede vi serveren her midlertidig her. Denne server installerede vi OSSEC IDs package og OSSEC klient agents på de andre maskiner, hvorefter de kommunikere sammen.

## 14.3 Sikkerhed

Vi vil i dette afsnit gå nærmere ind på implementering af sikkerhed i vores system.

### 14.3.1.1 Authentication

Vi har implementeret forskellige typer af authentication og brugerstyings systemer som er følgende underafsnit.

#### 14.3.1.2 Active directory

I Active Directory tilføjede vi en fælles accounts på et fælles domæne ved navn 4Semester.dk.

Vi har joinet alle interne servere på domænet 4Semester.dk undtagen Server 3 og Server 4.

De tilføjede fælles accounts i Active Directory systemet:

- **Brugernavn:** administrator – **Kodeord:** asd123! – Har adgang til alt
- **Brugernavn:** Nick – **Kodeord:** <ikke mulig> - Adgang til klient desktop
- **Brugernavn:** Kim – **Kodeord:** <ikke mulig> - Adgang til klient desktop

#### Udfordringer

- Vi er i tvivl om Server 3 kan joines på domænet, fordi Active Directory på Server 2 er afhængig af DHCP/NAT i Server 3.

#### Løsningsforslag

- Vi troede at Active Directory brugte krypteret forbindelser, men efter nærmere undersøgelse under implementering fandt vi ud af ved at læse dokumentationen nærmere, at forbindelserne ikke var krypteret. Så vi anbefaler stærkt at opsætte følgende under produktion.

#### 14.3.1.3 DHCP Server

Ved implementering af Windows Server 2012 R2 hypervisoren er der også tjek på om der kun findes en DHCP server i netværket med featuren DHCP guard.

#### 14.3.1.4 MAC address spoofing

Ved implementering af Windows Server 2012 R2 hypervisoren er der også beskyttelse for Mac address spoofing.

#### 14.3.1.5 Windows local accounts

Vi har implementeret default Windows lokal brugersystem for Server 3.

Vi har for Server3 lavet følgende lokale accounts:

- **Brugernavn:** VPN – **Kodeord:** asd123! – Adgang til netværket
- **Brugernavn:** administrator – **Kodeord:** asd123!

#### 14.3.1.6 Linux local accounts

Vi har implementeret en lokal account for IDS Ubuntu Linux serveren.

Vi har tilføjet følgende lokale accounts:

- **Brugernavn:** root – **Kodeord:** asd123! – adgang til alt

### 14.3.2 Kryptering

I dette afsnit går vi nærmere ind, hvilke steder vi har implementeret kryptering i systemet.

#### 14.3.2.1 VPN

VPN er sat op med default settings, Microsoft Point-to-Point Encryption (MPPE)

#### 14.3.2.2 Remote adgang

Vi har implementeret RDP data kryptering for kommunikationen imellem remote klient og interne servere. Server authenticationen derimod er TLS.

### 14.3.3 Isolering

Vi har brugt Virtualisering og virtuelle netværk, til at adskille og isolere.

#### 14.3.3.1 Virtualisering

Vi har implementeret ESXI 6 som den første virtuelle infrastruktur og brugt [ESXI software komponenter](#) til at kunne isolere hypervisor OS fra guest's OS.

Vi har derefter implementeret Windows Server 2012 R2 Hyper-V og [dens software komponenter](#) til at isolere vores system fra kunder og hver kunde fra hinanden.

#### 14.3.3.2 Data

Data isoleres ved hjælp af virtuelle harddiske for hver virtuel server.

#### 14.3.3.3 Virtuelle netværk

Vi har lavet virtuel netværk med vSwitch og machine port groups

**vSwitch0:** indeholder følgende machine port groups

**VM Network:** følgende VM's er tilknyttet dette netværk:

Server 3, Proxy(ikke i brug) med Vlan ID: All (4096).

**VM Network 3:** følgende VM's er tilknyttet dette netværk:

Server 1 med Vlan ID: 3

**VM Network 2:** følgende VM's er tilknyttet dette netværk:

Server 1, Server 3, server 2, Server 5, Proxy(ikke i brug) med Vlan ID: 2

**Storage VM:** følgende VM's er tilknyttet dette netværk:

VMK1 : 10.255.108.80 med Vlan ID: All(4096)

**VMKernel Port:** følgende VM's er tilknyttet dette netværk:

VMK0 : 10.255.108.80 med Vlan ID: All(4096)

### 14.3.4 IDS

Vi har implementeret IDS trejdepart OSSEC package i en nested virtuel Ubuntu server.

IDS'en skulle have været installeret kun som virtuel maskine på ESXI serveren fremfor den virtuelle Windows hypervisor.

### Forbedring

- Vi ønskede også at installere et web GUI med til OSSEC, men det lykkes også ikke i denne omgang at få installeret.

### 14.3.5 Anti virus

Vi har ikke prioriteret installation af anti-virus højt. Vi fandt ud at ESXI server har integrations muligheder for installation af anti-virus og Windows Server 2012 R2 hypervisor har default antivirus med sig.

#### 14.3.5.1 Windows Defender

Vi har som default for alle server aktiveret Windows Defender som antivirus program.

## 14.4 Availability

Vi har prioriteret remote adgang, fordi ifølge vores krav og design er vigtigt, for at kunne være fleksible.

### 14.4.1 Remote adgang

Vi har implementeret remote adgang til ESXI'en med vSphere. Remote adgang til server 3 via VPN, og her fra internt fjernskrivebord til samtlige andre interne server.

## 14.5 Performance

Vi har prioriteret performance, fordi ifølge vores krav og design er vigtig, men også fordi virtualisering kan reducere performance meget, hvis implementering ikke er konfigureret rigtig.

### 14.5.1 Elasticity

Vi har konfigureret ESXI serveren således, at alle vores virtuelle servere mindst har adgang til 2 virtuelle kerner. De har ikke nødvendigvis garanteret adgang hele tiden til de samme virtuelle kerner, men de virtuelle maskiner har adgang til 2 ud af 12 virtuelle kerner i en midlertidig periode.

Der er minimum 4 GB ram på alle virtuelle maskiner også, som automatiske tildeles løbende efter behov.

Server 1 derimod har vi tildelt flere virtuelle kerne og mere ram det er her kundernes VM's ligger nested.

ESXI hjælper med automatisk at skalere ressource forbruget, frem for manuel virtuel skallering. Dette kaldes [elasticity](#) når ESXI serveren gør det automatisk.

## 15 Final test

Vi vil i dette afsnit forklare de sikkerhedstest vi har lavet og test af funktionalitet.

### 15.1 Scanning

Her under viser vi resultatet at en ip range scan i Nmap fra kali linux. Vi bruger denne scanning til at teste, hvilke porte der er åben, og hvilke services der kører på de åbne porte. Denne scan viser tydeligt at vores servere er ret åben for angreb, især serveren med AD er ret åben, hvilket kan være en sårbarhed ved eventuelt angreb.

```
root@kali:~# nmap 192.168.1.*
```

```
Starting Nmap 7.01 ( https://nmap.org ) at 2016-06-05 04:25 EDT
```

```
RTTVAR has grown to over 2.3 seconds, decreasing to 2.0
```

```
RTTVAR has grown to over 2.3 seconds, decreasing to 2.0
```

```
Nmap scan report for 192.168.1.1
```

```
Host is up (0.087s latency).
```

```
Not shown: 990 filtered ports
```

```
PORT      STATE SERVICE
```

```
53/tcp    open  domain
```

```
80/tcp    open  http
```

```
135/tcp   open  msrpc
```

```
443/tcp   open  https
```

```
445/tcp   open  microsoft-ds
```

```
1723/tcp  open  pptp
```

```
49155/tcp open  unknown
```

```
49157/tcp open  unknown
```

```
49158/tcp open  unknown
```

```
49159/tcp open  unknown
```

```
Nmap scan report for 192.168.1.2
```

```
Host is up (0.0044s latency).
```

```
Not shown: 984 filtered ports
```

```
PORT      STATE SERVICE
```

```
53/tcp    open  domain
```

```
88/tcp    open  kerberos-sec
```

```
139/tcp   open  netbios-ssn
```

```
389/tcp   open  ldap
```

```
445/tcp   open  microsoft-ds
```

```
464/tcp   open  kpasswd5
```

```
593/tcp   open  http-rpc-epmap
```

```
636/tcp   open  ldapssl
```

```
3268/tcp  open  globalcatLDAP
```

```
3269/tcp  open  globalcatLDAPssl
```

```
49153/tcp open  unknown
```

```
49156/tcp open  unknown
```

```
49157/tcp open  unknown
```

```
49158/tcp open  unknown
```

```
49159/tcp open  unknown
```

```
49165/tcp open  unknown
```

```
Nmap scan report for 192.168.1.5
```

```
Host is up (0.024s latency).
```

Not shown: 994 filtered ports

PORT	STATE	SERVICE
135/tcp	open	msrpc
139/tcp	open	netbios-ssn
445/tcp	open	microsoft-ds
2179/tcp	open	vmrpd
49154/tcp	open	unknown
49156/tcp	open	unknown

Nmap scan report for 192.168.1.12

Host is up (0.0019s latency).

Not shown: 991 filtered ports

PORT	STATE	SERVICE
80/tcp	open	http
135/tcp	open	msrpc
443/tcp	open	https
445/tcp	open	microsoft-ds
1723/tcp	open	pptp
49155/tcp	open	unknown
49157/tcp	open	unknown
49158/tcp	open	unknown
49159/tcp	open	unknown

Nmap done: 256 IP addresses (4 hosts up) scanned in 355.19 seconds

## 15.2 Banner grapping

Her under vises en banner grapping ip scan lavet med Nmap i kali linux. Denne type scan giver til forskel fra en normal ip scanning også info omkring, hvilket os en given host har, hvilket giver mulighed for at finde eventuelle sårbarheder i det aktuelle OS.

```
root@kali:~# nmap -F -O 192.168.1.*
```

Starting Nmap 7.01 ( <https://nmap.org> ) at 2016-06-05 07:04 EDT

Nmap scan report for 192.168.1.1

Host is up (0.052s latency).

Not shown: 93 filtered ports

PORT	STATE	SERVICE
53/tcp	open	domain
80/tcp	open	http
135/tcp	open	msrpc
443/tcp	open	https
445/tcp	open	microsoft-ds
49155/tcp	open	unknown
49157/tcp	open	unknown

Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port

Device type: general purpose

Running: Microsoft Windows 2012

OS CPE: cpe:/o:microsoft:windows\_server\_2012



OS details: Microsoft Windows Server 2012

Nmap scan report for 192.168.1.2

Host is up (0.019s latency).

Not shown: 90 filtered ports

PORT	STATE	SERVICE
------	-------	---------

53/tcp	open	domain
--------	------	--------

88/tcp	open	kerberos-sec
--------	------	--------------

135/tcp	open	msrpc
---------	------	-------

139/tcp	open	netbios-ssn
---------	------	-------------

389/tcp	open	ldap
---------	------	------

445/tcp	open	microsoft-ds
---------	------	--------------

3389/tcp	open	ms-wbt-server
----------	------	---------------

49153/tcp	open	unknown
-----------	------	---------

49156/tcp	open	unknown
-----------	------	---------

49157/tcp	open	unknown
-----------	------	---------

Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port

Device type: general purpose

Running: Microsoft Windows 2012

OS CPE: cpe:/o:microsoft:windows\_server\_2012

OS details: Microsoft Windows Server 2012

Nmap done: 256 IP addresses (2 hosts up) scanned in 215.69 seconds

## 15.3 IDS detection

Vi har testet for OSSEC IDS for reaktioner på angreb, scanning, hoved ændringer i systemet eller forsøg på adgang til systemet. Vi testede på en nested virtuel maskine med installation af OSSEC agent og monitor software på en nested virtuel ubuntu maskine.

### 15.3.1.1 Stealth scan

Vi scannede på hele det interne netværk med nmap toolen i Kali linux v2 og fandt ud af at OSSEC ikke som default kunne detektere angrebet.

#### Anbefalinger

- Det er muligt at lave egne regler til følgende.

### 15.3.1.2 Fil ændringer

Ved brug af administrator rettigheder ændrede vi "C:\Windows\System.ini" på en virtuel Windows maskine med installation af OSSEC agent fra

```
; for 16-bit app support
[386Enh]
woafont=dosapp.fon
EGA80WOA.FON=EGA80WOA.FON
EGA40WOA.FON=EGA40WOA.FON
CGA80WOA.FON=CGA80WOA.FON
CGA40WOA.FON=CGA40WOA.FON

[drivers]
wave=mmdrv.dll
timer=timer.drv
[mci]
```

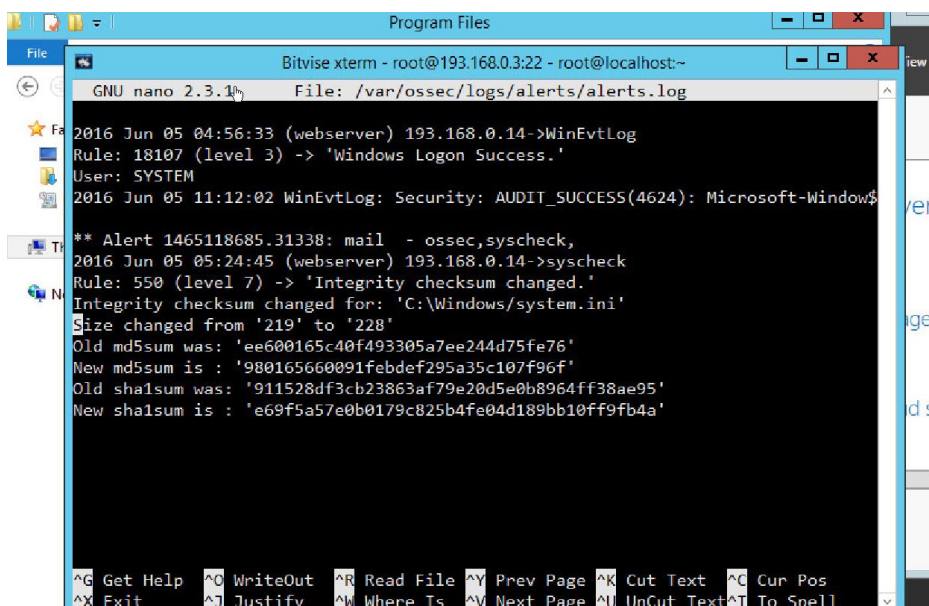
Til

```
; for 16-bit app support
[386Enh]
woafont=dosapp.fon
EGA80WOA.FON=EGA80WOA.FON
EGA40WOA.FON=EGA40WOA.FON
CGA80WOA.FON=CGA80WOA.FON
CGA40WOA.FON=CGA40WOA.FON

[drivers]
wave=mmdrv.dll
timer=timer.drv
test=test
[mci]
```

Vi kunne se at OSSEC fangede ændringen og advarede med level 7, at dette var sandsynligvis var skadelig for systemet.

Du kan se logfilen herunder fra OSSEC IDS serveren.

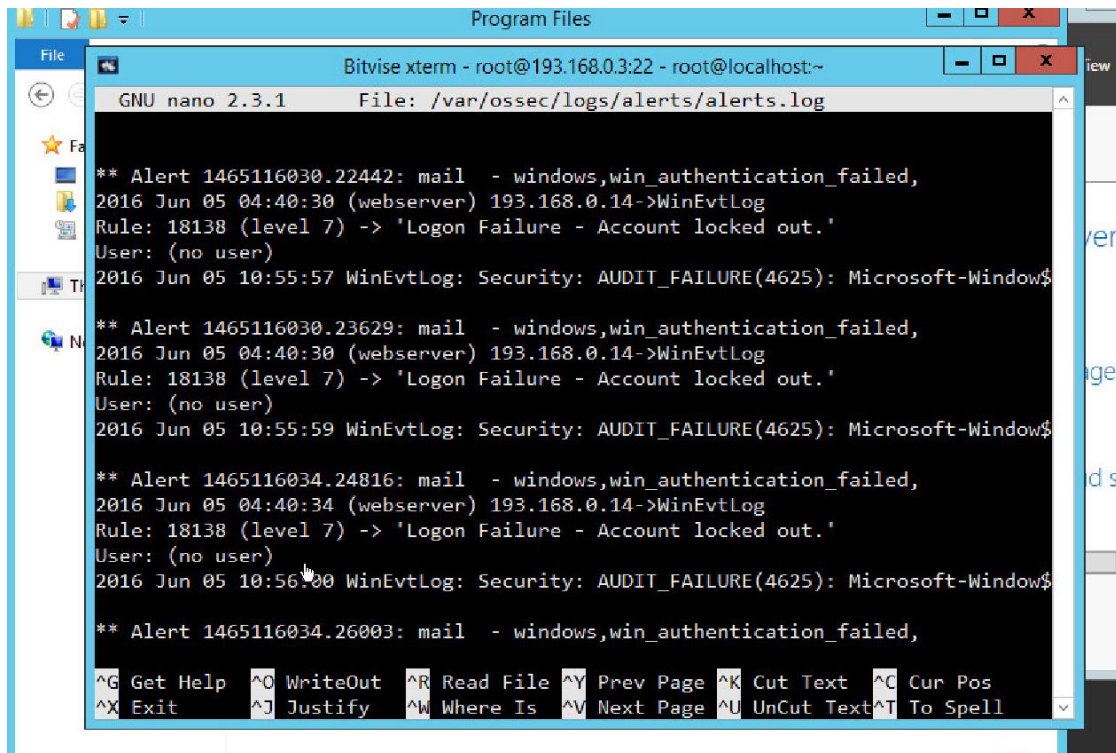


```
GNU nano 2.3.1 File: /var/ossec/logs/alerts/alerts.log
2016 Jun 05 04:56:33 (webserver) 193.168.0.14->WinEvtLog
Rule: 18107 (level 3) -> 'Windows Logon Success.'
User: SYSTEM
2016 Jun 05 11:12:02 WinEvtLog: Security: AUDIT_SUCCESS(4624): Microsoft-Windows$
** Alert 1465118685.31338: mail - ossec,syscheck,
2016 Jun 05 05:24:45 (webserver) 193.168.0.14->syscheck
Rule: 550 (level 7) -> 'Integrity checksum changed.'
Integrity checksum changed for: 'C:\Windows\system.ini'
Size changed from '219' to '228'
Old md5sum was: 'ee600165c40f493305a7ee244d75fe76'
New md5sum is : '980165660091febdef295a35c107f96f'
Old sha1sum was: '911528df3cb23863af79e20d5e0b8964ff38ae95'
New sha1sum is : 'e69f5a57e0b0179c825b4fe04d189bb10ff9fb4a'
```

### 15.3.1.3 Administrator adgang for Windows og Linux

Vi testede også ved forsøg på bruger adgang ved at indtaste forkert password op til flere gange for en administrator account på en virtual Windows maskine med OSSEC agent.

Vi kunne her se at OSSEC fangede det og sendte en advarsel til logfilen.



The screenshot shows a Bitvise xterm window with a nano 2.3.1 editor open to the file /var/ossec/logs/alerts/alerts.log. The log contains four alerts, each indicating a 'Logon Failure - Account locked out.' for the user '(no user)' on 2016 Jun 05. The alerts are triggered by 'windows,win\_authentication\_failed' and 'WinEvtLog: Security: AUDIT\_FAILURE(4625): Microsoft-Windows\$'. The xterm window title is 'Bitvise xterm - root@193.168.0.3:22 - root@localhost:~'.

```
GNU nano 2.3.1 File: /var/ossec/logs/alerts/alerts.log

** Alert 1465116030.22442: mail - windows,win_authentication_failed,
2016 Jun 05 04:40:30 (webserver) 193.168.0.14->WinEvtLog
Rule: 18138 (level 7) -> 'Logon Failure - Account locked out.'
User: (no user)
2016 Jun 05 10:55:57 WinEvtLog: Security: AUDIT_FAILURE(4625): Microsoft-Windows$

** Alert 1465116030.23629: mail - windows,win_authentication_failed,
2016 Jun 05 04:40:30 (webserver) 193.168.0.14->WinEvtLog
Rule: 18138 (level 7) -> 'Logon Failure - Account locked out.'
User: (no user)
2016 Jun 05 10:55:59 WinEvtLog: Security: AUDIT_FAILURE(4625): Microsoft-Windows$

** Alert 1465116034.24816: mail - windows,win_authentication_failed,
2016 Jun 05 04:40:34 (webserver) 193.168.0.14->WinEvtLog
Rule: 18138 (level 7) -> 'Logon Failure - Account locked out.'
User: (no user)
2016 Jun 05 10:56:00 WinEvtLog: Security: AUDIT_FAILURE(4625): Microsoft-Windows$

** Alert 1465116034.26003: mail - windows,win_authentication_failed,
```

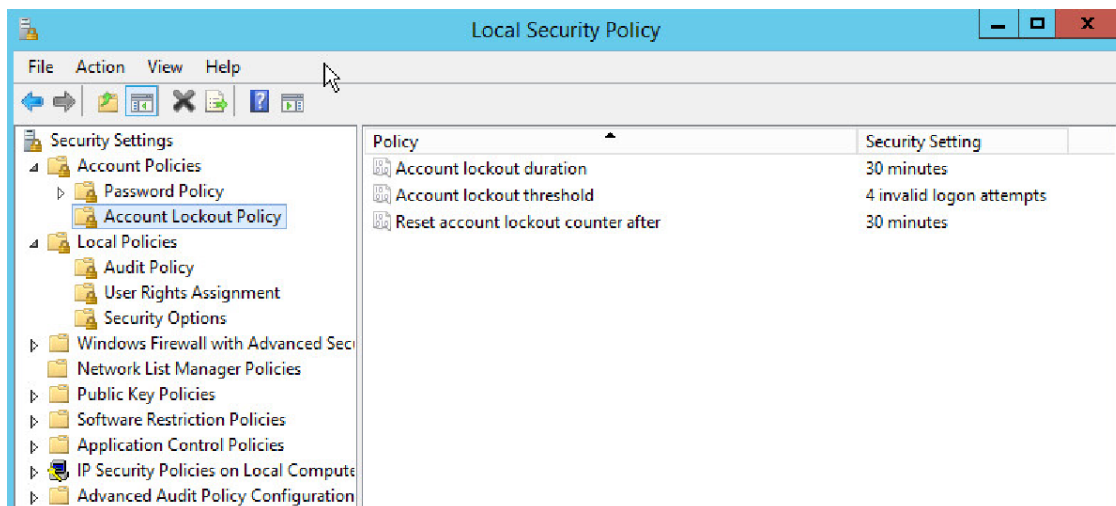
## 15.4 Uautoriseret adgang

Vi testede vores system for ekstern uautoriseret adgang ved manuelt forsøge at logge ind på virtuelle servere.

### 15.4.1 VPN test

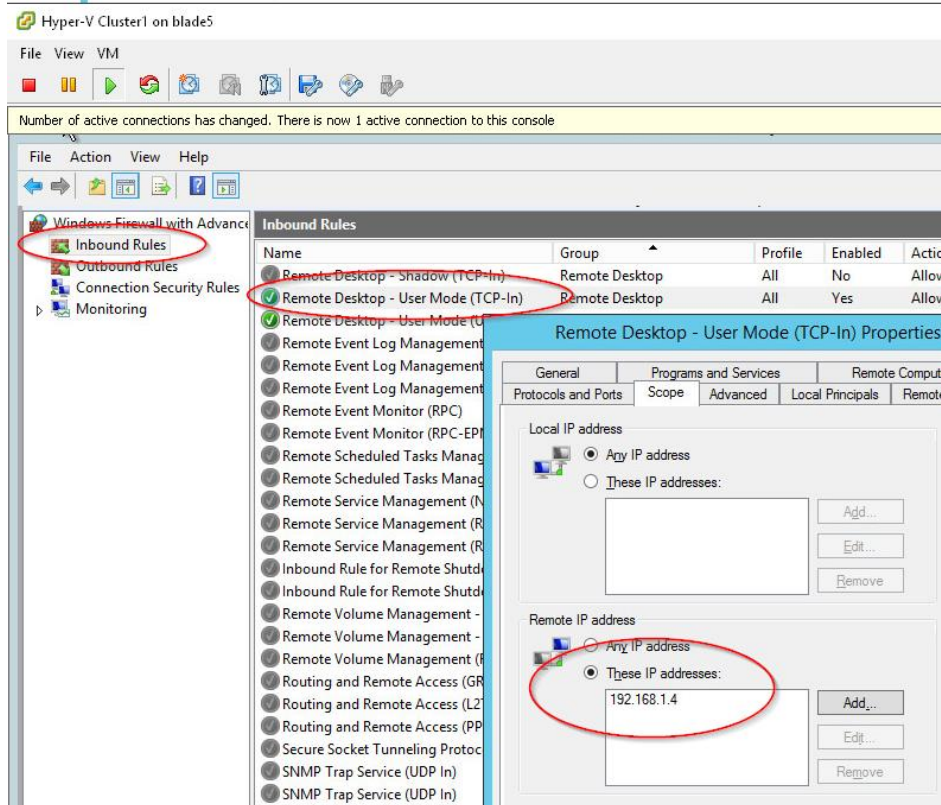
Vi testede om VPN lokal account for Server 1 låste sin account ved for mange forkerte password indtastninger.

Vi havde indstillet policy til at, hvis administrator account blev indtastet forkerte 4 gange låses account. Det virkede!



### 15.4.2 Firewall test

Vi mener også at firewalls er et must i alle systemer da dette er med til at filtrere en del af den trafik der tilgår systemet. Samt bruges til at lukke af for porte og services der ikke bruges, da disse oftest er en stor sikkerheds risiko hvis de ikke bliver lukket. Som vist på billedet her under har vi lukket for remote desktop i firewallen for eksterne kilder, men har lavet en undtagelse for en intern ip 192.168.1.4 som er vores remote client.



Efterfølgende forsøgte vi at remote til serverne fra en ekstern kilde for at teste at dette ikke var muligt med succes da dette ikke var muligt. Vi har også teste at vores undtagelse for den interne ip virkede, og vi havde fuld remote adgang til samtlige servers fra den interne ip.

## 16 Studie profiler & baggrund

Her kan i se vores studieprofiler.

### 16.1 Nick Reese profil

Mit mål med Projektet var at få mere viden og forståelse for:

- Virtualisering og Cloud computing
- Windows Server 2012 R2 og Microsoft teknologier
- Vsphere/EXSI og VMWare teknologier
- VPN

for at forbedre min forståelse for arkitekturen bag applikationerne, samt administrationen af disse applikationer for at sikre bedst muligt drift og sikker tilgang til systemet for at undgå uautoriseret adgang.

### 16.2 Kurser

<b>System administration</b>	<p>Mit fokus under forløbet var at få indsigt i og basal viden om Windows server 2012 R2, da dette er oftest brugt i erhvervslivet og af almene folk, min erfaring jeg har fået under forløbet har jeg så brugt i praksis i vores projekt</p> <p>Brug i projektet: Gjort brug af hyper-v virtualiserings tool, NAT, DHCP, Active directory, DNS, server administration</p>
<b>Security</b>	<p>Jeg har under dette forløb fået udvidet min viden omkring risikoen ved at have servers online eller i det hele taget være koblet på internettet.</p> <p>Brug i projektet: Vurdering af hvordan systemet skulle sættes op, tools til pentesting, overvejelser af trusler mod systemet.</p>
<b>Web development ASP.NET</b>	<p>Jeg har under dette forløb opnået kendskab til blandt andet, Bootstrap, restfull API, MVC, generelle CMS systemer, samt bedre forståelse for integration af webløsninger.</p> <p>Brug i projektet: Senere brug af integrationer til eventuelle webløsninger, og evt. brug af API, samt overvejelser for arkitektur valg og infrastruktur valg.</p>
<b>android</b>	<p>Jeg har under dette forløb erfaret at det er meget komplekst, og at min interesse for emnet er meget mangelfuld.</p>

#### Passion

Jeg brænder for spil udvikling, og har gjort brug af Unity udviklings tool. Og selv om jeg godt kunne tænke mig at blive ansat som udvikler i et firma som udvikler spil, jeg har dog erfaret af dette er uhyre svært at komme til at arbejde inden for og har derfor valgt at ligge mit fokus på system administration, og vil gerne lære mere om at håndtere sikkerhed.

#### Uddannelse

<b>2014</b>	<b>Web-integrator</b> Tech College Aalborg
<b>2017</b>	<b>Datamatiker</b> University College Nordjylland

## 16.3 Kim Dam Grønhøj profil

Mit mål for dette projekt var, at få mere viden og forståelse for

- Virtualisering og Cloud computing
- Windows Server 2012 R2 og Microsoft teknologier og arkitektur
- Vsphere/EXSI og VMWare teknologier og arkitektur
- Praktisk brug af hosting teknologier

så jeg bedre kan forstå arkitekturer bag software applikationer, og hvordan sikres softwareløsninger bedst muligt i både drift og mod uautoriseret adgang.



## 16.4 Kurser

### **System administration**

Mit fokus under forløbet var, at få basal viden om Windows Server 2012 R2 arkitektur og praksis brug af Hyper-v, Active directory, IIS og Windows licens services. Jeg fik også inspiration til Microsoft SQL Server enterprise features. Jeg lærte også om teoretisk viden og begreber, hvordan CPU, ram, harddiske spiller sammen, og hvordan virtualisering fungerer i dybden.

#### **Hvad kan jeg bruge det til, i projektet?**

Til at bruge Windows platformen til private clouds, backups, NAT, DHCP, DNS, VPN, server administration policies, identity og authentication solution.

### **Web development ASP.NET**

Mit fokus var at få inspiration i nye web teknologier, og hvorfor jeg skulle vælge bestemte teknologier frem for andre i forhold til vedligeholdelse og lave nye produkter. Jeg lærte om de forskellige CMS systemer (Umbraco, Wordpress osv) kan bidrage med for sig i dag, end for 5 år siden. Jeg fik også bedre forståelse for REST FULL API modellen.

#### **Hvad kan jeg bruge det til, i projektet?**

Til at tænke bedre valg af virtuel infrastruktur og arkitektur med at integrere et REST FULL API senere.

### **Using databases**

Jeg lærte flere begreber og design regler for databaser og hvilke fordele der i Mongoddb i forhold til at hoste big data.

#### **Hvad kan jeg bruge det til, i projektet?**

Det har ikke været aktuelt at bruge det i projektet, men det har givet tanker til, hvor man burde placere sin data servere henne i virtualisering.

### **Security**

Jeg fik en bedre forståelse for, at social engineering hurtigt kan blive et problem i en virksomhed. Jeg fik også afprøvet hacking tools (Kali linux) i praksis. Så at jeg i dag ved som udvikler, hvor hurtigt en black hacker kan finde informationer om bestemte servere uden at have adgangskoder, samt hvor meget information de kan få ud af en virksomhed uden virksomheden ved, at black hackere er ved at gøre sig klat til et attack. Jeg fik også inspiration til, hvilke overvågningsværktøjer der findes. Dette forløb har været det mest lærerige for mig på 4. semester. Det var meget udfordrende.

#### **Hvad kan jeg bruge det til, i projektet?**

Til at kunne teste vores server setups sikkerhed, og hvilke værktøjer vi kan bruge til at monitor et netværk angreb og hvordan vi kan undgå det bedst mulig.

## 16.5 Passion

Jeg kunne godt tænke mig, at blive ansat i en virksomhed, som arbejder med virtualisering, automatisering af tests (unit test) og komplekse integrationsløsninger til større mængder data med PHP, ASP.NET, Xamarin og Windows/Linux løsninger. Gerne en virksomhed som har fokus på, at vedligeholde deres systemer løbende, frem for at lave et produkt til en kunde, levere det og installation og ikke længere vedligeholder det efterfølgende.

## 16.6 Uddannelser & kurser

<b>2009</b>	<b>Web-integrator</b> Tech College Aalborg
<b>2014</b>	<b>Iværksætter kursus</b> Aalborg kommune
<b>2015</b>	<b>Wiindows Server introduktion</b> edx.org
<b>2017</b>	<b>Datamatiker</b> University College Nordjylland



## 17 Konklusion

Vi konkludere, at ESXI 6 fra VMWare er et godt valg til at implementere sikker virtualisering, fordi de har mange flere features der kan hjælpe med at beskytte mod trusler og sårbarheder og er det eneste nuværende virtualisering software vi har kunne finde der understøtter nested virtualisering.

Vi har valgt nested virtualisering, fordi det giver mulighed for test miljø og mulighed for opgradering af hypervisor der reducere nødvendigheden for hardware køb og nedetid.

Et forsøg på at forhindre trafikovervågning er vSwitchs, virtuel port groups og VLANs til at opnå isolering af netværket i form af reduceret tilgængelighed af datapakkerne. Vi har erfaret at det ikke er muligt 100% at forhindre trafikovervågning.

Vi har fundet ud af det er muligt at reducere effektiviteten af DDOS angreb ved brug af Load balance i vSwitchs, ethernet adapters og automatisk ressourcestyring af CPU og RAM for de virtuelle maskiner.

For at opnå sikker remote adgang til vores system er VPN i godt værktøj til kryptere forbindelsen og lave en ekstra dør/lag til systemet, som låses ved for mange forkerte indtastninger. Så i alt er der 3 dører/lag ind til systemet, som er VPN, desktop klient og efterfølgende remote til serverne.

Hyper-v fra Microsoft er godt på vej til at blive et godt valg også, samtidig med integrationerne til Microsoft produkter er rigtig godt.

## 18 Perspektivering

Vi burde fra start have været bedre til at undersøge, hvilke hardware krav der stilles til datacenter og virtualisering. Vi vil gerne have opsat og implementeret ligesom vores design valg og arbejdet mere med IDS og penetration testing.

## 19 Procesrefleksion

Vi kan sige at krav og virkelig er langt fra hinanden, fordi vi synes sikkerhed for virtualisering er meget komplekst at opsætte og vedligeholde.

Vi synes det var svært i starten på grund af forvirring af forskellen mellem virtuel infrastruktur og arkitektur.

Under design og implementering syntes vi, at vi fik en bedre forståelse.

Det kræver store mængder tid ved problemer og tilføjelse af nye features, samt det kan være meget testkrævende og tidskrævende at sikre systemet er sikkert.

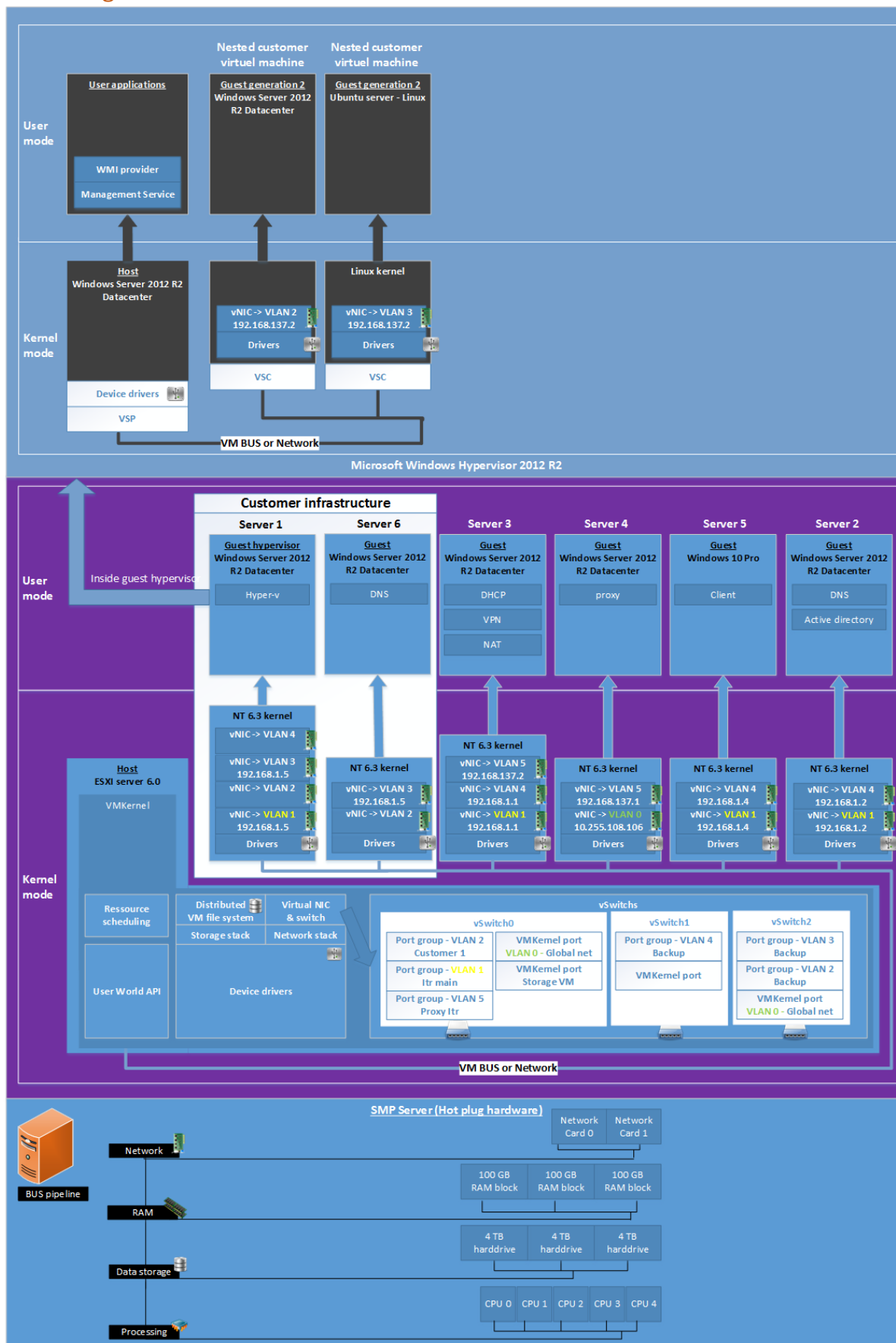
## 20 Litteraturliste

1. Operating Systems: Internals and Design Principles



## 21 Bilag

### 21.1 Bilag 1



## 21.2 Billag 2

Nmap ip range scan, Command: nmap 192.168.1.\* scanned in 586.68 sekunder

192.168.1.1

Port	State	Service
53/tcp	Open	Domain
80/tcp	Open	http
135/tcp	Open	Msrpc
443/tcp	Open	https
445/tcp	Open	Microsoft –ds
1723/tcp	Open	Pptp
49155/tcp	Open	Unknown
49157/tcp	Open	Unknown
49158/tcp	Open	Unknown
49159/tcp	Open	Unknown

192.168.1.5

Port	State	Service
135/tcp	Open	Msrpc
139/tcp	Open	Netbios –ssn
445/tcp	Open	Microsoft –ds
2179/tcp	Open	Vmrpd
49155/tcp	Open	Unknown
49157/tcp	Open	Unknown

192.168.1.11

Port	State	Service
135/tcp	Open	Msrpc
139/tcp	Open	Netbios –ssn
445/tcp	Open	Microsoft –ds

192.168.1.12

Port	State	Service
80/tcp	Open	http
135/tcp	Open	Msrpc
443/tcp	Open	https
445/tcp	Open	Microsoft –ds
1723/tcp	Open	Pptp
49155/tcp	Open	Unknown
49157/tcp	Open	Unknown
49158/tcp	Open	Unknown
49159/tcp	Open	Unknown

## 21.3

### 21.4 Bilag 3

#### Interview med Kasper Nielsen

16. marts

16-03-2016 14:04

Nick Reese

hvad gør i med sikker hed Kasper ??

16-03-2016 14:04

Kasper Horsfeldt Nielsen

Mht?

16-03-2016 14:05

Nick Reese

datacenter, og jeres virtuelle servers

16-03-2016 14:22

Kasper Horsfeldt Nielsen

datacentret har vi som sådan ikke noget med at gøre, da vi bar lejer pladsen

de virtuelle maskiner blander vi os ikke i, det er fuldt unmanaged vi sælger, så der er ikke noget sikkerhed fra vores side, end ikke firewalls eller noget

16-03-2016 14:23

Nick Reese

ja okay

så jeres er rent opsætning af VM's ?

så i er bare mellem mænd ?

16-03-2016 14:23

Kasper Horsfeldt Nielsen

i stedet for at bruge tid på at beskytte os, så kan de kun tilgås fra vores interne IP netværk, som igen kun kan tilgås af den unikke vpn id jeg har

det kan man godt kalde os ja :)

16-03-2016 14:25

Nick Reese

hvorfor har i valgt at bruge VPN ?? og hvordan er det opsat ?? vi har fået af vide vpn er outdatet ?

og bruge i DHCP server ?

16-03-2016 14:27

Kasper Horsfeldt Nielsen

nope, eller dvs vi bruger kun dhcp til vores dedicated maskiner

alle VPS'er får en fast static ip tildelt direkte på router niveau

vi bruger vpn fordi det er beregnet til præcis det som vi bruger det til.. alle servernes management del af på en fast IP: 172.16.1.x

men for at tilgå de IP'er, så skal man være logget på VPN og have tildelt en IP fra 172.16.1.x netværket

16-03-2016 14:29

Nick Reese

okay :D

takker :D

16-03-2016 14:29

Kasper Horsfeldt Nielsen

på den måde, så er vi helt sikker på at eventuelle bøller skal have fat i vores vpn key først, som kun findes på min og min partners pc, derefter skal de så bryde koden til vpn'en som automatisk spærrer efter 3 forsøg, men lykkes det, så skal de bryde koden på serverne, som også spærrer efter 3 forsøg

16-03-2016 14:30

Kasper Horsfeldt Nielsen

ud fra det, så tør jeg godt stå inde for at det ik sker :D

16-03-2016 14:31

Nick Reese

så man kan remote serveren ??

16-03-2016 14:31

Kasper Horsfeldt Nielsen

fra vpn ja

via command line, vi har ingen gui på serverne

16-03-2016 14:32

Nick Reese

okay :D

16-03-2016 14:32

Kasper Horsfeldt Nielsen

Vedhæftet fil ikke tilgængelig

Denne vedhæftede fil er måske blevet fjernet, eller den person, der har delt den, har måske ikke tilladelse til at dele den med dig.

16-03-2016 14:32

Kasper Horsfeldt Nielsen

det er en video af en maskine lige pt, som er ved at reinstall :D

16-03-2016 14:32

Nick Reese

send link :D

16-03-2016 14:33

Kasper Horsfeldt Nielsen

sku være sendt her

:P

men er ik nået frem endnu ser det ud til

16-03-2016 14:33

Nick Reese

intet

hehe

16-03-2016 14:34

Kasper Horsfeldt Nielsen

sender lige igen

16-03-2016 14:34

Nick Reese

har i sql og web server på samme maskine ??

takker :D

16-03-2016 14:35

Kasper Horsfeldt Nielsen

0:14

16-03-2016 14:35

Kasper Horsfeldt Nielsen

vi har sql på alle maskinerne

men kun én server til webhosting

som så godt nok også have sql på samme maskine, men det er nu lige så meget fordi den fint kan trække det :P

16-03-2016 14:36

Nick Reese

hvad gør i mod DDoS ?

16-03-2016 14:36

Kasper Horsfeldt Nielsen

intet

venter på det er væk

:P

16-03-2016 14:36

Nick Reese

okay hvorfor ?

bruger i ikke Proxyes ?

16-03-2016 14:37

Kasper Horsfeldt Nielsen

proxies kan slet ik klare det vi bliver ramt af :P

hvis de rammer en enkelt node, så skal de op omkring 40Gbit før den begynder at være sløv

16-03-2016 14:37

Nick Reese

hvor meget bliver i angrebet ??

16-03-2016 14:37

Kasper Horsfeldt Nielsen

og tæt på 100Gbit før den er offline

hele infrastrukturen kan æde ca 500Gbit uden at gå ned

16-03-2016 14:38

Nick Reese

hold da op :O

16-03-2016 14:38

Kasper Horsfeldt Nielsen

skal vi beskytte os imod ddos større end det, så skal vi op i nogle afsindige priser

vores client panel bliver ramt dagligt :P

men det rører den ik rigtigt

16-03-2016 14:38

Nick Reese

okay

16-03-2016 14:39

Kasper Horsfeldt Nielsen

hvis de giver den rigtig god gas så kan den godt være lidt sløv

men så skal de også have mange bots

16-03-2016 14:39

Nick Reese

hvad er der er tools til at sikre mod DDoS osv ? vi skal ikke bruge priser men tools :D

16-03-2016 14:39

Kasper Horsfeldt Nielsen

det er lidt det, der er ik rigtig noget

vi bruger fail2ban

sammen med nginx ratelimits

16-03-2016 14:40

Nick Reese

okay :)

16-03-2016 14:40

Kasper Horsfeldt Nielsen

det som det gør, er at hvis en IP forsøger at loade siden mere end x gange i minuttet, så bliver den bannet i 24 timer

det kan tage toppen af det, men hvis angrebet er omfattende nok

så kan vi ikke rigtig gøre noget :P

16-03-2016 14:41

Nick Reese

okay

16-03-2016 14:41

Kasper Horsfeldt Nielsen

men de skal virkelig have noget at give af for at ligge webserveren ned

kan klarer snildt et par millioner requests i minuttet :D

16-03-2016 14:41

Nick Reese

nice :)

16-03-2016 14:42

Kasper Horsfeldt Nielsen

2 users, load average: 1.60, 1.62, 0.77

vi er faktisk under angreb lige nu :P

16-03-2016 14:42

Nick Reese

køre i med antivirus på maskinerne ??

16-03-2016 14:42

Kasper Horsfeldt Nielsen

munin melder ~500k hits

næ.. det er linux? :D

16-03-2016 14:43

Nick Reese

hvad med fil serverne ?

eller mail servers?

16-03-2016 14:43

Kasper Horsfeldt Nielsen

vi driver ik mail servers for andre

16-03-2016 14:43

Nick Reese

hvor ofte opdatere i ?

16-03-2016 14:44

Kasper Horsfeldt Nielsen

vi bruger clamav på vores interne mail

der pushes updates ud

så de kommer når de bliver udgivet

16-03-2016 14:44

Nick Reese



okay

hvordan sikre i interne servers mod at angribe hinanden ?

eller at en intern server bruges mod jer ?

16-03-2016 14:46

Kasper Horsfeldt Nielsen

en intern server kan kun nåes og bruges via vores vpn netværk

man kan ik få adgang til styresystemet eller lign uden vpn

16-03-2016 14:47

Nick Reese

har hver private cloud VMderes egen firewall ?

16-03-2016 14:47

Kasper Horsfeldt Nielsen

hvis kunden vil have det ja :p

vm niveauet sikrer at de ik kan komme ind i selve maskinen

16-03-2016 14:48

Nick Reese

bruger i VMware ?

hvis jeg har lejet en VM maskine af jer hvordan får jeg så adgang til den og kan jeg se de andre VM i har ?

16-03-2016 14:49

Kasper Horsfeldt Nielsen

nej vi bruger proxmox

du får tildelt en ip, som du kan forbinde til

du kan ingen steder se hvor mange eller hvem som er på maskinen

16-03-2016 14:50

Nick Reese

okay :D

har i et VLAN for hver VM ??

16-03-2016 14:51

Kasper Horsfeldt Nielsen

nope

16-03-2016 14:52

Nick Reese

okay mange tak :D

har hver VM så dens egen VPN, altså er den installeret på VM eller hvor køre den henne ??

16-03-2016 14:53

Kasper Horsfeldt Nielsen

kunderne har ik nogne vpn

de har bar direkte adgang til nettet

det er kun til hostnodes som der kræves vpn

16-03-2016 15:51

Nick Reese

17. marts

17-03-2016 12:09

Nick Reese

laver i threat analyse ? og hvordan ??

17-03-2016 12:15

Kasper Horsfeldt Nielsen

threat analyse af hvad?

17-03-2016 12:16

Nick Reese

i går fortalte du i var under angreb af DDoS

hvad er de største threats mod jer ?

osv

17-03-2016 12:18

Kasper Horsfeldt Nielsen

nej det går vi ik op id

id = i

17-03-2016 12:18

Nick Reese

okay :)

30. marts

30-03-2016 10:17

Nick Reese

hvordan ser jeres infrastruktur / arkitektur ud ? :D

30-03-2016 11:24

Kasper Horsfeldt Nielsen

hvordan ser jeres infrastruktur / arkitektur ud ?

hvad tænker du der?

30-03-2016 11:26

Nick Reese

Jamen det lidt svært :-/ hvordan er jeres hardware sat op / samme. Og hvordan er den virtuelle del opdelt osv?

30-03-2016 11:27

Kasper Horsfeldt Nielsen

pretty basic

proxmox ve 4.1 på alle nodes, installeret på et usb stick

selve hardwaren varierer lidt..

men generelt dual 10 core cpu, 512-1024GB ram, 24 til 90x512G SSD

storage nodes er dual 10 core, 256-512G ram og 90x4TB disk

30-03-2016 11:31

Nick Reese

Nodes?

30-03-2016 11:32

Kasper Horsfeldt Nielsen

ren shared nodes er mindre, typisk dual 8 core, 128g ram og 24x4T

1 server = 1 node :P

30-03-2016 11:32

Nick Reese

Er jeres hardware koblet sammen via lan vabler eller via bus?

Kabler\*

30-03-2016 11:33

Kasper Horsfeldt Nielsen

2x10Gbit netværk

der er ingen direkte forbindelser mellem serverne, det er der ingen grund til, de udveksler nærmest ingen data

30-03-2016 11:34

Nick Reese

Så det er ikke sat op som en stor fælles resourse?

30-03-2016 11:34

Kasper Horsfeldt Nielsen

nej, det er for dyrt

30-03-2016 11:34

Nick Reese

Okay :-)

30-03-2016 11:34

Kasper Horsfeldt Nielsen

hver maskine hoster en pulje kunder

er der nogle problemer så kan vi jo flytte dem til en ny server

midlertidigt.

30-03-2016 11:35

Nick Reese

Hvordan holder i overblik over systemet ?

30-03-2016 11:36

Kasper Horsfeldt Nielsen

proxmox :)

de er alle en del af et cluster derinde

30-03-2016 11:36

Nick Reese

Okay

30-03-2016 11:36

Kasper Horsfeldt Nielsen

som giver fine grafer osv

30-03-2016 11:36

Nick Reese

Okay Nice :-)

Jeres skæler ikke automatisk så?

30-03-2016 11:38

Kasper Horsfeldt Nielsen

folk kan instant upgrade/downgrade lige som de har lyst til

30-03-2016 11:38

Nick Reese

Okay

Hvis en kunde vil upgrade ud over den maskine de ligger på skal i så skal i selv flytte dem ?

30-03-2016 11:41

Kasper Horsfeldt Nielsen

korrekt

så bliver den flagged og så flytte vi den

30-03-2016 11:42

Nick Reese

Ja okay

30-03-2016 11:42

Kasper Horsfeldt Nielsen

men det sker nærmest aldrig

tror ikke vi har haft nogen i år

30-03-2016 11:42

Nick Reese

Okay

30-03-2016 12:29

Nick Reese

ved du hvad det hedder når mere en en CPU deler bus ??

30-03-2016 12:50

Kasper Horsfeldt Nielsen

hvilken sammenhæng?

30-03-2016 12:52

Nick Reese

tror vi har fundet det Symmetric multiprocessing

30-03-2016 13:26

Kasper Horsfeldt Nielsen

Irrelevant i forhold til hosting

04-05-2016 08:57

Nick Reese

Hey champ hvad hedder dit firma egentligt ? :D

04-05-2016 10:16

Kasper Horsfeldt Nielsen

Hvilket af dem? :p

Hvis du bliver kunde så vil det være i hnielsen networks

04-05-2016 10:18

Nick Reese

Hvad skal vi henvise til i form af vi har brugt dig som rådgiver :-P

04-05-2016 10:18

Kasper Horsfeldt Nielsen

Hnielsen networks

Det er den danske afdeling

25-05-2016 10:53

Nick Reese

hey hvordan fordeler i globale IP adresser ud til de VMs kunderne har ??

25-05-2016 10:54

Kasper Horsfeldt Nielsen

det håndterer solusvm selv

25-05-2016 10:54

Nick Reese

solusvm ?

det er det datacenter i køre igennem ?

25-05-2016 10:55

Kasper Horsfeldt Nielsen

det er det kontrolpanel som vi bruger backend til at styre alle vms

25-05-2016 10:55

Nick Reese

ahh okay

25-05-2016 10:55

Kasper Horsfeldt Nielsen

sammen med proxmox som kan det samme

25-05-2016 10:55

Nick Reese

på den måde

25-05-2016 10:55

Kasper Horsfeldt Nielsen

IP'erne er announced hos vores upstream providers

25-05-2016 10:57

Nick Reese

okay

Management client giver ikke mening får assigned IP'er. Der må være en server/router som får dem alle tildelt

25-05-2016 11:02

Kasper Horsfeldt Nielsen

de er bare announced hos upstream, når de gør det. så kan alle vores servere dynamisk bruge en ip indenfor det range

har vi fx 1000 IP'er announced i holland

så kan vi uanset hvilken server, bare dynamisk tildele den/de ip'er vi vil have til en enkelt maskine

25-05-2016 11:03

Nick Reese

hvordan sikre i så en anden ikke får en forkert IP-adresse.

det er ikke ISP som kender alle jeres maskiner. Der må være noget imellem som bestemmer fordelingen

25-05-2016 11:34

Kasper Horsfeldt Nielsen

Det gør solus.