Har du råd til at lade være?
- Sådan overlever du ransomware.

Flere og flere danske virksomheder bliver ramt af ransomware angreb, det er i dag ikke et spørgsmål om, hvorvidt din infrastruktur rammes, men hvornår.

Med de budgetter og opgaver IT afdelingerne i dag skal håndtere og de mange opgaver der skal prioriteres, er der ikke midler nok til at sikre sig mod 100% mod et angreb og udfordringen for os er at vi kan ikke sikrer os mod malware før det er kendt af producenterne, så på et eller andet tidspunkt vil vi blive ramt.

I dette whitepaper viser vi hvorledes du kan sikrer dit IT-miljø, således at skaden bliver mindst mulig, når du bliver ramt, samt sikrer at systemerne kan komme tilbage til operativt niveau hurtigst muligt, baseret på teknologier der tilgængelige i dag.

Det skulle have været en helt almindelig fredag på kontoret for IT-chef Konrad Mikkelsen.[1]

Morgenen var startet som vanligt derhjemme, kaffe med fruen, en tur med hunden og så lige ind og tjekke om der var nogle gode tilbud på nettet, det var jo Black Friday.

Andre have fået samme idé som Konrad, flere sider var nede og man skulle tro verden var ved at gå under sådan som alle talte om Black Friday.

Turen til kontoret startede fint og Konrad sad i køen på motorvejen og tænkte over alle de projekter hans afdeling havde haft gang i henover året, da hans mobil ringede.

Det var chefen…

Og på ganske få minutter blev det i sandhed en sort fredag for IT-chef Konrad Mikkelsen.

Chefen havde også handlet via nettet på Black Friday og havde fået en mail med et super tilbud fra en anderkendt webshop, som han havde åbnet på sin maskine på kontoret og nu kunne han ikke få adgang til sin computer, den var låst og hans password virkede ikke.

Da Konrad afsluttede opkaldet lå der 5 nye beskeder på hans telefon, han skyndte sig at ringe tilbage til Lonnie som var system administrator og som lød lidt stresset på beskeden, noget om en masse brugere der ikke havde adgang til deres systemer.

Efter at have talt sammen om hvad brugerne havde oplevet var Lonnie og Konrad ikke længere i tvivl om hvad der var ved at ske… De var ramt af en cryptolocker og et hurtigt tjek på storage systemet viste også en masse aktivitet som ikke var normal og bekræftede dem i deres frygt.

Heldigvis var et af årets gennemførte It-projekter en opdatering af deres gamle infrastruktur, hvor de udskiftede deres rackservere og gamle diskhylder og båndstationer, med et tidsvarende og moderne datacenter, hvor de også benyttede sig at ekstern back-up ude i ”skyen”.

Samtidig havde de fået etableret en disaster/recovery plan i samarbejde med deres it samarbejdspartner, en plan som de også havde testet, i lyset af de mange ransomware sager Konrad Mikkelsen havde læst om i pressen og hørt om på sine møder med andre IT chefer.

Planen var forholdsvis simpel og nem at forstå og eksekvere, i grove træk følger den reglerne fra helt almindelig førstehjælp, som de fleste kender og kan huske når panikken breder sig:

Stands ulykken

Giv livredende førstehjælp

Tilkald hjælp

Giv almindelig førstehjælp

[1] Konrad Mikkelsen er en fiktiv person, handling og løsning er dog baseret på virkelige hændelser hos danske kunder.

Stands ulykken, luk systemerne ned, således at angrebet begrænses, dette indebærer også at stoppe alle backup jobs, således at backup ikke inficeres.

Giv livredende førstehjælp, gennemgå alle centrale systemer og tjek seneste ikke inficerede back up for status.

Tilkald hjælp, inddrag de nødvendige eksterne specialister der skal til for at få renset systemet samt få etableret normal drift igen

Giv almindelig førstehjælp, centrale systemer re-etableres fra back-up og normal drift etableres, samtidig med devices tjekkes og re-etableres i prioriteret orden.

For Konrad Mikkelsen betød det at hans sorte fredag blev til langfredag.

Fredag aften var 75% af systemer i normal drift og mandag morgen var alle brugere og systemer i normal drift.

Hvordan var dette muligt?

I dette whitepaper vil vi beskrive teknologier og metoder der gør dette muligt for de fleste IT afdelinger.

Men inden først 3 gode råd …

Betal aldrig

Anmeld altid

Husk at tage back-up og teste den

Hvad er Ransomware

Ordet Ransomware er en sammentrækning af de engelske ord Ransom (Løsesum) og Software og i praksis betyder det et stykke program/software som er lavet for at afpresse brugere en løsesum for igen at få adgang til data.

Ransomware kommer i mange afarter og kvaliteter og med lige så mange forskellige påvirkninger af din infrastruktur og programmer. Ransomware er blevet speciel populær blandt IT-kriminelle de seneste 5 år og der er masser af eksempler på såvel storstilede angreb som mere målrettede angreb også her i Danmark, hvor især den offentlige sektor har været udsat. Eller rettere, hvor især den offentlige sektor har talt åbent om at have været angrebet. Desværre virker angrebene også på den måde at virksomheder ikke ønsker at fortælle offentligt om at de har været udsat for angreb… måske fordi skaden er sket og man ikke ønsker sit omdømme og kundernes tillid udsat for spekulationer. Hvilket bringer os tilbage til de 3 gode råd, fra tidligere.

Hvordan virker Cryptolocker

Et af de mest udbredte Ransomware værktøjer i øjeblikket er Cryptolocker, som kort fortalt virker ved at der eksekveres et program som krypterer filer ved hjælp af en 2048 bit RSA nøgle, bestående af 2 nøgler, en public og en privat.

Public nøglen er den som krypterer filer i den ramte enhed og private nøglen er den som IT piraten har og er den eneste nøgle som kan låse de nu krypterede filer op. I praksis har vi set organisationer hvor programmet spreder sig fra fileshare til fileshare via netværksdrevene i en virksomhed med katastrofale følger. Virksomheder bliver lammet når det ikke er adgang til burgernes og applikationernes fildrev, som jo nu er krypteret.

Et cryptolocker angreb er fra IT piratens side fulgt op med et krav om løsesum for at frigive den private RSA nøgle som kan låse filerne op, normalt ved at den ramte virksomhed sender en af krypterede filer til IT piraten og får den tilbage i ukrypteret tilstand.

Det nemmeste nu er at betale IT piraten og få nøglen, således at alle filer låses op.

Samtidig er det, det værste at gøre, derved anspores IT Piraten til at fortsætte sine ugerninger samt vi hjælper med at finansiere kriminaliteten.

Men hvad gør man så?

Udover at få det anmeldt, således at myndighederne og sikkerhedsvirksomhederne har et overblik over omfanget og måske får en chance for at fange nogle af disse IT pirater, så det allervigtigste at STOPPE ulykken for at begrænse skaderne. Simultant iværksættes ens disaster/recovery procedurer, (for sådan en har man forhåbentligt, ellers er det om at få sat en i værk)

Hvordan kommer man af med Cryptolockeren og får genetableret normal drift?

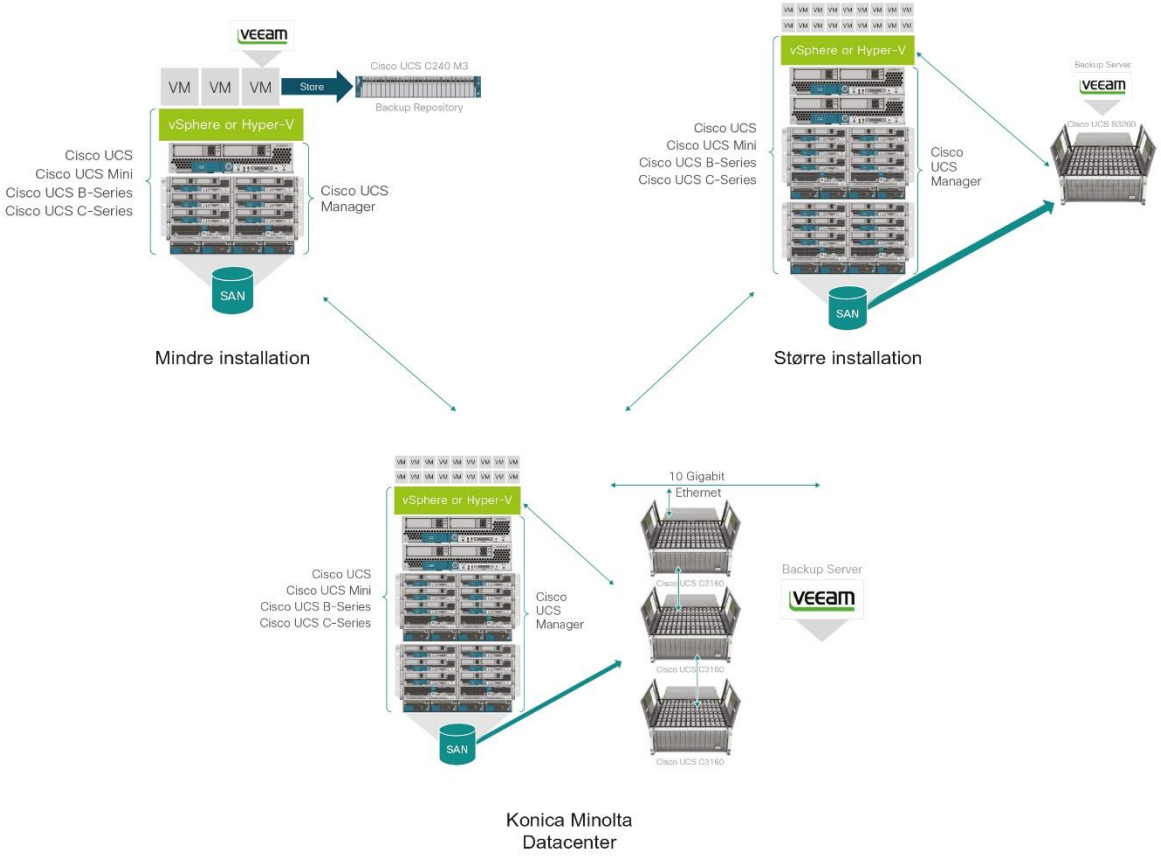
Lad os vende tilbage til Konrad Mikkelsen og se hvad han gjorde.

Men inden lad os lige se på hvordan Konrad Mikkelsens datacenter infrastruktur ser ud, som nævnt tidligere har Konrad Mikkelsen fået opdateret sit Datacenter til et moderne datacenter, med produkter som arbejder tæt sammen i et virtualiseret og automatiseret datacenter baseret på en FlexPod arkitektur.[2]

Flexpod er et arkitektur samarbejde mellem Cisco (Netværk og servere) og NetApp (Storage) og i Konrad Mikkelsens datacenter består Flexpodden også af Vmwares hypervisor og Veeam software, alt sammen bygget over et Cisco/NetApp valideret design, endvidere har Konrad Mikkelsen valgt Back-up as a Service hos Konica Minolta, baseret på Veeam.

Figuren nedenfor viser hvorledes Konica Minoltas BackUp as a Service, med Veeam er opbygget.

[2] www.cisco.com/go/flexpod



Figur 1: Konica Minolta BackUp as a Service baseret på Veeam Cloud connect

Hvordan Black Friday blev til en lang fredag.

Det første Konrad Mikkelsen gjorde, efter at have konstateret de var ramt af en cryptolocker, sammen med sine IT folk var at isolere problemet, standse ulykken, ved at lukke ned for mailsystemet og netværksdrevene, således at angrebet kunne standses. Alt sammen i henhold til den Disaster/Recovery plan som var blevet etableret tidligere på året og testet sammen med Konica Minoltas konsulenter. Dette betød også at back-ups blev gennemgået for at finde ud af hvor hårdt ramt man var, med andre ord, hvornår i tid har vi en pålidelig back-up som ikke er inficeret. Da Konrad Mikkelsen back-up er baseret på Veeam og NetApps snapshots er det muligt at have back-ups med ned til 5 minutters interval.[3]

Efter at have identificeret en brugbar back-up kom turen til servermiljøet, det nemmeste i denne situation var en re-installation, for at sikre et så rent miljø som muligt. Da Cisco UCS er baseret på virtuelle instanser af de fysiske servere (Service profiler) var servermiljøet oppe at køre igen

[3] https://www.veeam.com/netapp-snapshot-snapvault-snapmirror-integration.html

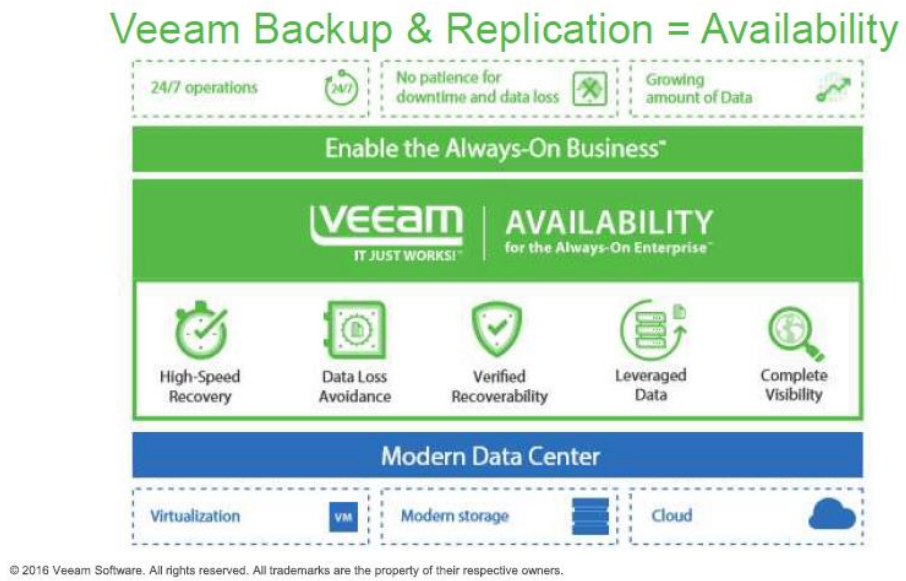
indenfor en time, dernæst kunne Veeams Back-Up images rulles på og endelig kunne miljøet testes inden endelig idriftsættelse og genetablering af databaser.

For Konrad Mikkelsen og hans team betød det at hele infrastrukturen var operationel og i normal drift inden kl 20 fredag aften, med kun 5 timers nedetid og mindre end 2 timers datatab.

Lidt mere om nogle af de valgte teknologier i Konrad Mikkelsens Datacenter

VEEAM

Som beskrevet ovenfor er det tydeligt at Veeam backup og replication funktionalitet er en af nøglerne til at dette var muligt. På figuren nedenfor ses hvordan Veeam passer ind i det moderne datacenter.



Figur 2: Veeam Availabilty Suite 9.5

I vores case med Konrad Mikkelsen består det moderne datacenter af en FlexPod med Vmware som Hypervisor, NetApp storage og Cisco servere og netværk.

De 5 hovedelementer i Veeams availability suite som gjorde det muligt at etablere normal drift så hurtigt var:

High Speed Recovery, som består af en række underliggende værktøjer som gør det muligt at have en RTO (Recovery Time Objective) på under 15 minutter i nogle tilfælde endog helt ned til

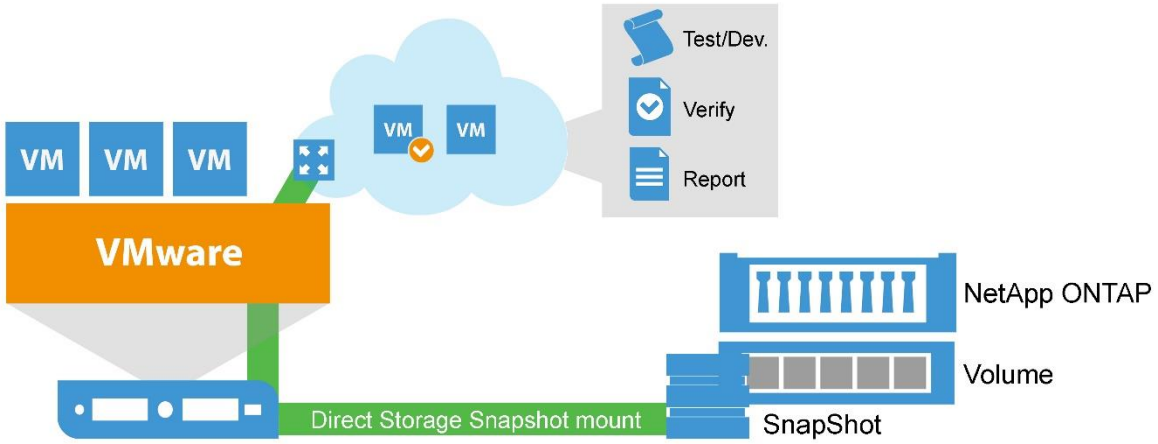
2 minutter. Et af værktøjerne er *Instant VM Recovery*, der som navnet antyder gør det muligt at afvikle en virtuel maskine direkte fra en back-up, uden først at skulle have lavet en recovery af denne. Et andet værktøj er *Instant File-Level Recovery*, der gør det muligt at gendanne enkelt filer uden at re-etablere virtuelle disk mm først. Endelig er der *VEEAM Explorers* samlingen som er udviklet med henblik på at kunne restore enkelte elementer inde fra applikationer som: Oracle, Micrososft Active Directory, Microsoft Exchange, Microsoft Sharepoint, Microsoft SQL og endelig *Storage Snapshots* til eksempelvis NetApp for at kunne restore enkelte filer eller hele VMs fra et back-up snapshot.

Data Loss Avoidance, er en lang række værktøjer der skal sikre os imod datatab og samtidig giver os en RPO (Recovery Point Objective) på under 15 minutter. For at sikre en så god RPO selv i store miljøer har Veeam udviklet *automatic intelligent load balancing* og *built-in WAN acceleration*, hvor *automatic intelligent load balancing* gør præcis som navnet siger balancere workloads intelligent i vores infrastruktur. Dette sikres dels ved at Veeam selv vælger den rigtige proxy til at køre wokloadet igennem men også ved at iops nok til back-up jobbet ved at udnytte Veeams egen patenteret BackUp I/O control for at sikre at produktionsmiljøet ikke påvirkes af back-up miljøet. *Built-in WAN acceleration* giver os mulighed for at flytte vores data til egne remote datacentre eller evt. Konica Minoltas datacenter op til 50x hurtigere end ved rå datatrafik hastighed. Veeams integreret WAN accelerator gør det nemt og sikkert at sikre os en hurtig recovery med en lav RPO.

Verified Recoverability, er din sikkerhed for at backup faktisk virker, ifølge en undersøgelse[4] er det kun ca. 5% af backups der testes for om de virker, med Veeams *SureBackup* startes din backup i et isoleret virtual lab og funktionalitet mm. testes og der sendes en statusrapport til din mailadresse. *SureReplica* er din sikkerhed for de forskellige replica af dine backups virker, på samme måde som *SureBackup*, startes en replica op i et isoleret Virtual lab og testes, hvorefter der sendes en status rapport.

Leveraged Data betyder at vi skal have mere ud af vore data og i denne tid hvor big data bliver en større del af alle IT installationer, er det vigtigt at have værktøjer som gør det muligt at få udnyttet de mange data vi har i vore systemer. Hos Veeam giver *Leveraged Data* dig en række værktøjer som gør det muligt at arbejde med data i et isoleret miljø og er velegnet til at skabe kopier af dit driftmiljø og kan med fordel benyttes test af disaster/recovery planer ved at oprette et *Virtual Lab*, således at du ikke påvirker produktions data og miljø.

[4] Veeam datacenter availability report 2014



Figur 3: Veeam Virtual Lab

I Veaams *Virtual Lab* booter du direkte fra dine backup og kan arbejde i enten et *On-Demand Sandbox* miljø eller et *On-Demand Sandbox for Storage Snapshots* miljø. *On-demand Sandbox* er velegnet til at teste applikationer mm. Inden man sætter dem i drift, samt giver mulighed for at træne og uddanne folk i et near-live drift miljø og meget mere. *On-Demand Sandbox for Storage Snapshots* giver os mulighed for at arbejde med produktions data i et sikkert miljø, afteste funktionaliteter og meget mere på ægte data, uden at kompromitere vores produktions miljø.

Complete Visibility er det sidste element i Veeams availability suite og et af de vigtigste i den daglige drift, da det er her vi får overblikket og hjælpen til at optimere vores Veaam miljø. Med udgangspunkt i Veeam ONE og de værktøjer der er til monitorering og kapacitets planlægning har vi en lang række dashboards og rapporter som hjælper med at giver dagligt overblik, samt en række intelligente forecast værktøjer med ”what-if” scenarier til at hjælpe os med den fremtidige opsætning og drift af vores datacenter.

Hvad er en Flexpod

FlexPod er ud over et meget tæt samarbejde mellem Cisco og NetApp (et samarbejde der går tilbage til NetApps opstart) også markedets førende converged infrastruktur løsning, med mere end 100 validerede designs bagved. En FlexPod består af 3 hovedkomponenter, en compute platform (Cisco UCS), en fabric platform (Cisco Nexus) samt en Storage platform (NetApp).

Fælles for dem alle er at der er et fælles management interface i en FlexPod, som gør det nemt at planlægge/installere, provisionere samt håndtere løsningen.

De mange validerede designs gør at der næsten altid er en FlexPod løsning der passer til ens behov, med udgangspunkt i et valideret design.

UCS Director som er grundpillen i management delen af en FlexPod betyder at den daglige drift af løsningen bliver nemmere end hvad vi kender til i dag.

Endelig betyder muligheden for fælles support at uanset hvilket problem der måtte opstå med en FlexPod vil der være adgang til den fælles support, som ud over den fysiske hardware også dækker afhjælpning/identificering af fejl på hypervisorer, samt OS og applikationer (såfremt disse er en del af et valideret design)

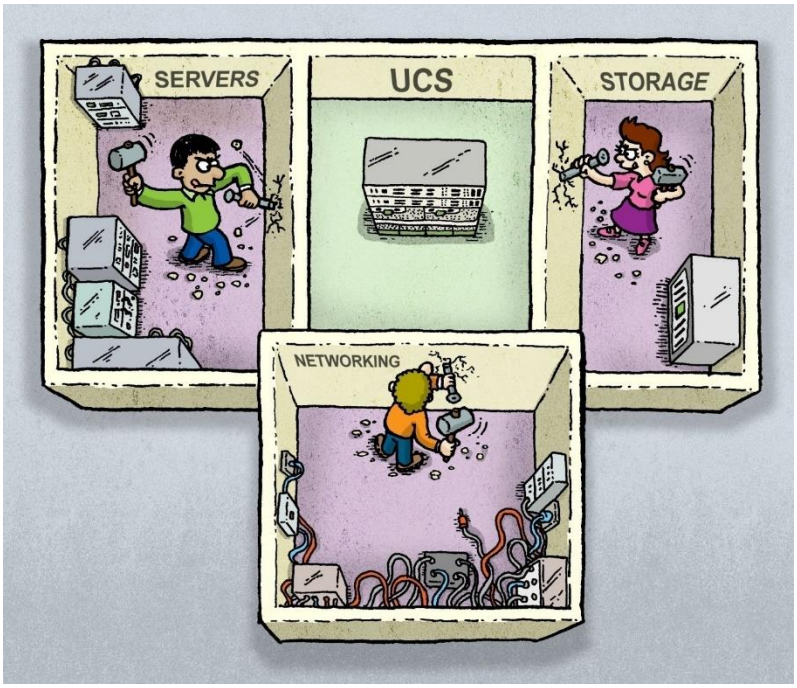
Hvad er Cisco UCS

Ciscos tilgang til datacentret er baseret på at platformene skal være velegnet til virtualisering og nemme at styre i hverdagen (easy-management) og dette ses tydeligt i Ciscos UCS arkitektur.

UCS står for Unified Computing System og siden Cisco meldte sig ind i server markedet i 2009 har markedet og samarbejdspartnerne taget godt imod UCS platformen og tankegangen bagved.

Cisco UCS er bygget op om 3 hovedplatforme som forener vores datacenter platforme i et system som er Unified, nemlig Unified Fabric, Unified Compute og Unified Management og hovedtanken bag dette er at vi skal have brudt siloerne i datacentret ned og være klar til det nye moderne datacenter, som udover at være virtualiseret også er automatiseret og i høj grad klar til at indgå i en eventuel Hybrid Cloud løsning.

Med andre ord er det skridtet på vej mod et software defineret datacenter og vores egen Private Cloud.



Figur 4: Cisco nedbryder datacenter siloerne

Unified management er nøglen til at vi kan styre og kontrollere vores infrastruktur og på Cisco UCS er det grundlæggende værktøj UCS Manager[5], som er værktøjet der styrer vores Unified Computing System (UCS), hvilket betyder såvel compute som fabric/netværks platformene håndteres fra et og samme interface. Det betyder at den daglige drift, gående fra konfigurering, provisionering, overvågning, fejlfinding og udbedring sker fra en og samme platform. Samtidig er det gennem UCS Manager at ekstern overvågning kan faciliteres, således at fejlalarmer mm kan sendes eksternt til Konica Minolta og/eller Cisco TAC support (Technical Assistance Center), således at den daglige drift afhjælpes.

UCS Manager er en domæne manager, hvilket betyder at for hvert UCS miljø man har, er der også en UCS Manager, da denne er integreret i de Fabric Interconnects der styrer UCS. Såfremt man har flere UCS miljøer kan man med fordel benytte UCS Central som er en global UCS manager (Manager of Managers), som er samme interface som UCS Manager, men er en virtuel manager.

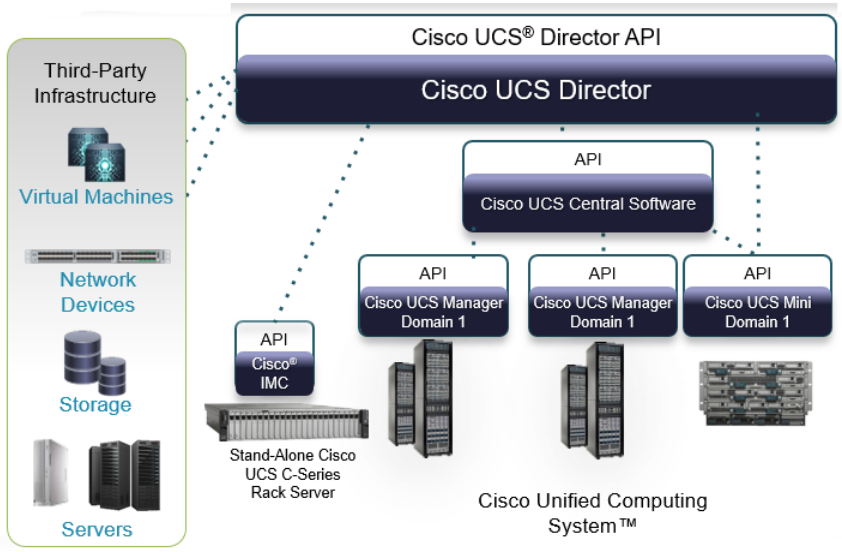
Her kan man udnytte at UCS Central og Manager er fuldt integreret således at man kan benytte globale profiler i sit management setup og kan vælge at have fuld gennemsigtighed på såvel compute som fabric platforme og konfigurationer.

UCS Manager integrerer med andre management platforme som eksempelvis VCenter fra Vmware og Microsoft System Center, i begge disse kan UCS manager styres via et plug-in, således at man ikke nødvendigvis skal tillære sig flere nye værktøjer.

Såfremt man ønsker at styre andet end Cisco hardware eller ønsker at opbygge et service katalog er management platformen UCS Director værktøjet.[6]

UCS Director arbejder sammen med en lang række 3. parts management platforme, hvilket betyder at UCS Director også er den management platform som styrer en Flexpod løsning, da den håndtere såvel CISCO UCS, Cisco Nexus som NetApp platformene gennem et og samme interface. Derudover kan UCS Director også styrer en lang række andre platforme. (Eks. EMC, IBM, HDS m.fl.)

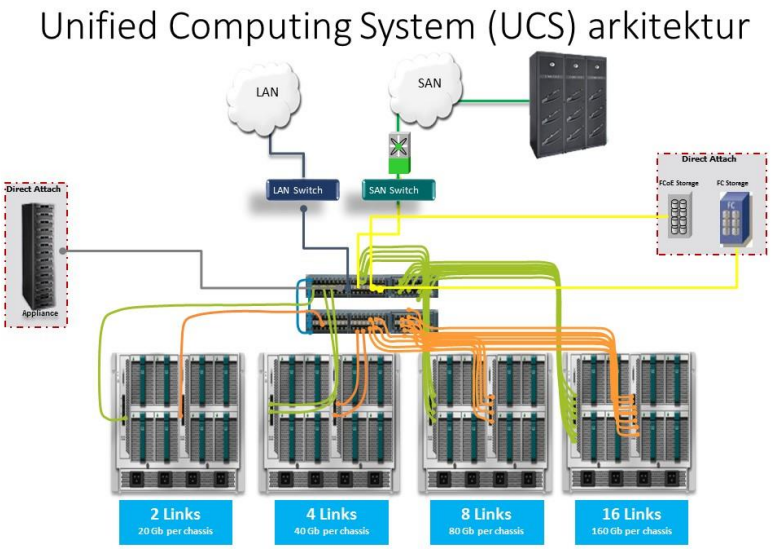
[5] http://www.cisco.com/c/en/us/products/servers-unified-computing/ucs-manager/index.html
[6] http://www.cisco.com/c/en/us/products/servers-unified-computing/ucs-director/index.html



Figur 5: Ciscos System management tilgang

Unified Computing er en af de andre byggestene i et UCS og her ses det tydeligt at Cisco har haft stor nytte af at have designet sin server platform med henblik på virtualisering.

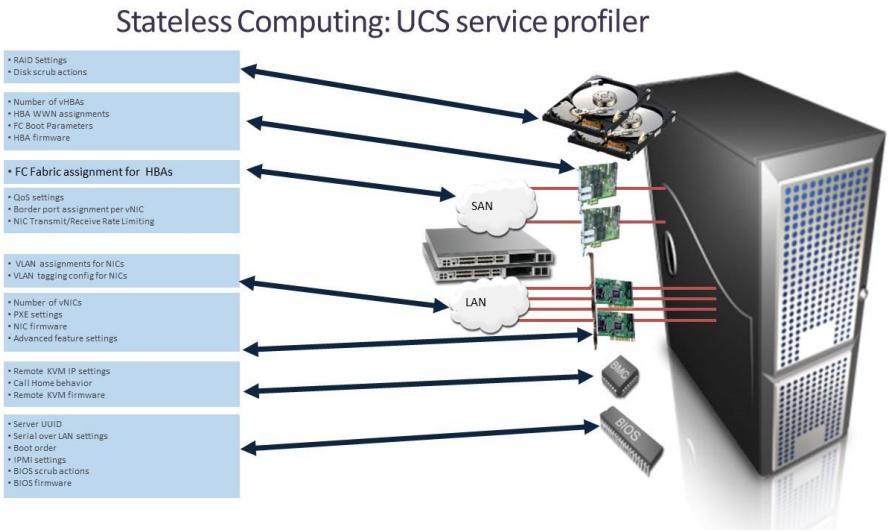
Der er 2 vigtige elementer i designet af en UCS server, der skal være tilgang til så meget memory som muligt, således at virtualiseringsgraden kan øges, samtidig med at der er så få mekaniske komponenter som muligt for at minimere fejlmuligheder i systemet. Endvidere skal man have fleksibilitet og skalerbarhed i sit miljø, skalerbarheden er sikret via brugen af 2 stk Fabric Interconnects (for redundans), herved kan der skaleres til 20 Blade Chasisser (160 Blades) samt utallige rackserver (bestemmes af hvor mange porte der er ledige på Fabric Interconnects), alle servere styres og håndteres gennem en og samme UCS Manager.



Figur 6: Cisco Unified Computing System (UCS) skalerbarhed og enkelthed

Fleksibiliteten sikres gennem brugen af service profiler, som er det ypperste indenfor Stateless Computing. Stateless Computing betyder at vi har en compute platform hvor vi er uafhængige af den fysiske platform og derved kan flytte rundt på vores server instanser uafhængigt af den underliggende platform og den dertil hørende fabric/kabling.

I Cisco UCS håndteres dette ved hjælp af service profiler, som er en virtuel version af de attributter/indstillinger vi normalt kender fra en fysisk server. Det betyder at vi går fra at konfigurere vores fysiske enhed til at bygge virtuelle instanser som dernæst lægges ud/påtrykkes vores fysiske enheder. Fordelene ved dette er mange, først og fremmest giver det os konsistens og sikkerhed, da vi ved at lave en master service profil har styr på versionsstyring af firmware, BIOS, netværk, SAN, memory, og meget andet (Se figur med service profil for eksempler på elementer der håndteres gennem service profil).



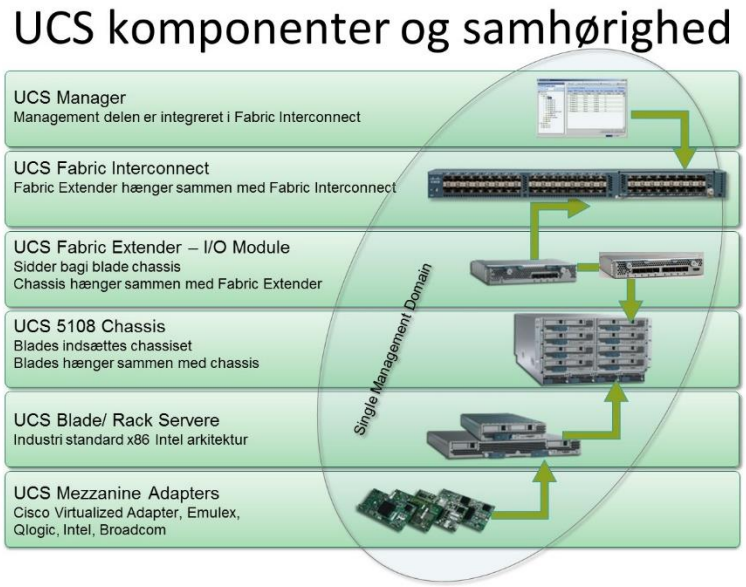
Figur 7: Cisco serviceprofil sikrer fleksibilitet og mobilitet i datacenteret

En anden fordel er at UCS manager som vi styrer vores miljø igennem, automatisk trækker den serviceprofil vi har defineret og lægger ud på den rigtige fysiske platform og derved giver den de egenskaber vi har defineret gennem service profilen, endelig giver stateless computing os en hurtig recovery tid såfremt vi rammes af nedbrud, da vi ”blot” skal have hardware reetableret og dernæst kan skubbe vores virtuelle miljø ud på den fysiske platform og være i drift igen i løbet af ganske kort tid.

Ydermere vil udvidelse af vores miljø kunne ske på ganske få minutter, da UCS Manager vil detektere såfremt en ny server er sat på systemet og dernæst pushe den profil ud på platformen som vi har defineret passer til denne (eks. Vmhost lille, Vmhost stor, Exchange, SQL osv.) og dernæst kan de sidste tilpasninger ske manuelt, såfremt dette er nødvendigt.

Unified Fabric er den sidste byggesten i UCS og en af grundende til at vi kan udnytte Stateless Computing til at gøre den daglige vedligeholdelse og drift nemmere end vi tidligere har kunnet på de traditionelle x86 platforme. Det starter i Fabric Interconnects som har Unified Porte, således at de nordpå kan kobles op imod en bestående fabric uanset om denne er Ethernet

(10/100 Mb, 1/10/40 GbE) eller FCAL (1/2/4/8/16 og 31Gb), på nogle systemer endog som direct attached storage dvs uden en SAN fabric.



Figur 8: Cisco UCS komponeter

Trafikken sydpå, ind i chassis og tilgangen til Blades sker via fabric extenders og på selve serveren sidder der en virtualiserings adapter (populært kaldet en VIC), Ciscos egen udviklet VIC kan håndtere op til 256 samtidige virtuelle adaptere og det er her at Stateless Computing virkelig gør en forskel, for når UCS først er kablet op, kan man via sin service profil altid ændre en konfiguration af en server, ved blot at udskifte service profilen, som indeholder konfigurationen på VIC og derved giver os det antal adaptere vi har defineret i vores service profil.

Nu kan du teste det selv, Konica Minolta tilbyder i samarbejde med Cisco og Veeam at du selv kan afprøve en back-up og replication løsning fra Cisco og Veeam i dit eget driftmiljø.

Konica Minolta kommer og sætter Cisco serveren op og i samarbejde med jer installerer og konfigurerer vi Veeam i jeres miljø og dernæst har i op til 90 dage at evaluere hvorvidt det er noget for jer, undervejs afholder vi evaluerings møder og sikrer at i får afprøvet Veeams funktionaliteter i jeres miljø. Når try & buy perioden er udløbet kan i vælge at købe systemet, såfremt i ikke vælger dette kommer vi og afinstallere og nedtager systemet igen.

Du kan se meget mere om løsninger fra Konica Minolta og vores partnere på:

www.elastiskinfrastruktur.dk

www.hyperflex.dk