

Sikkerhed Gennem Digital Transformation & Cloudmigration

De største udfordringer er nøglen til de største gevinster.

Gribes processen rigtigt an, og hvis de nye muligheder, der åbner sig ved at gå i clouden, udnyttes fuldt ud, vil virksomheder i processen kunne skabe nye rammer og præmisser for governance, compliance og budgetstyring, så bedre kontrol og mere sikkerhed bliver kombineret med og driver øget agilitet, værdiskabelse og innovation.

.....

“I clouden er disse nemlig ikke hinandens modsætninger, men gensidigt fremmende.”

I dette white paper ser vi på:

.....



Sikkerhed & Risiko:

Grundlæggende sikkerhed, compliance, ansvarsfordeling og migrationsproces.



Agilitet & Innovation:

I clouden kan kontrol og sikkerhed sætte kræfterne fri.



Skalerbarhed & Ressourceudnyttelse:

Ikke for meget, ikke for lidt og aldrig forgæves.



KEYCORE

Cloud Specialister

Indholdsfortegnelse

Intro	2
Sikkerhed & Risiko	4
Skyhøj Sikkerhed.....	5
Sikkerhed i Cloudmigrationens 4 faser.....	8
CASE: Pharmacovigilance, Sikkerhed & Compliance	9
Agilitet & Innovation	9
Paradigmeskift til DevOps.....	12
Fail fast. Don't break anything.....	12
CASE: PoC banede vejen til AI, ML og massive besparelser	12
2 X Hurtig, Sikker, og Effektiv Agilitet & Innovation	13
1. Automatisering med templates.....	15
2. Den digitale slikautomat: Landing Zone.....	16
CASE: Time-to-market in no time	17
Skalérbarhed & Ressourceudnyttelse	19
Elastik i metermål.....	19
De 3 Elasticiteter	20
Op.....	20
Ned.....	20
I anvendelse.....	20
Sikker Økonomi i Clouden	21
På et splitsekund.....	21
Indblik & Overblik.....	21
Kontrol & Skalering	22
Planlagt.....	22
Forudset.....	22
Dynamisk.....	22
Kontakt KeyCore	23

Intro

Digitaliseringsguruer og tech-giganter som Singulaity University, Facebook og Google har turneret med mottoer som "Disrupt or be Disrupted" og "Move fast and break things". Hvis man ikke vil blive overhalet indenom af born digital-upstarts, må man som virksomhed adoptere det agile, innovative imperativ og springe fremad imod Nirvana i clouden.

Og det vil formentlig være svært at finde en CxO, der direkte vil erklære sig som modstander af øget digitalisering. Digitaliseringen er et faktum, og alle vil også på et overordnet plan nikke anerkendende til, at det vil styrke virksomhedens evne til at innovere, indtage nye markeder og speede time-to-market-processerne op, hvis man bevæger sig væk fra den traditionelle entreprisemodel.

Det siger eksperterne, og i overskrifter eller strategi-power points er det svært at være uenig.

I virkelighedens verden forholder det sig dog anderledes. Og i forhold til den tilsyneladende udbredte konsensus, er det påfaldende så få virksomheder, der reelt og helhjertet har gennemført de store digitale transformationer.

I en undersøgelse foretaget af blandt andre Analyse Danmark tilkendegiver 32 procent af de adspurgte danske SMV'er, at de ikke anvender cloudløsninger, og hele 57 procent af de små virksomheder har heller ingen planer om det.

Bekymringer for sikkerheden går igen som årsag til at fravælge clouden.

Dette er dog hverken forbeholdt Danmark eller SMV'er. I en nyligt offentliggjort undersøgelse fra McKinsey¹ peger omkring 50% af CIOs i 52 af verdens største virksomheder på manglende evne til at sikre compliance og sikkerhed som den største barriere for den digitale transformation. Hvilket i samme undersøgelse også afspejler sig i, at blot 19% af de adspurgte CIOs anser digital transformation og en plads i clouden som en måde at opnå mere sikkerhed.

Det er, hvad vi kan læse ud af undersøgelser og suveys. Vores erfaring er dog, at sikkerhed i betydningen risikohåndtering og forsvar imod angreb ikke står alene som barriere for fuld cloudtransformation. Sikkerhed i betydningen kontrol og styring vejer lige så tungt. Agilitet og skalerbarhed lyder godt, men de kan være svære at indpasse med behovet for governance, compliance og ikke mindst faste og forudsigelige budgetrammer.

Dette er et paradoks.

¹ <https://www.mckinsey.com/business-functions/mckinsey-digital/our-insights/unlocking-business-acceleration-in-a-hybrid-cloud-world>

Dels giver digital transformation til cloud nemlig ikke bare adgang til risikohåndtering og forsvar imod angreb, der langt overgår, hvad vi kender fra traditionel on-premise eller warehouse-hosting.

Forudsætningen er, at det gribes rigtigt an.

Men perspektiverne er samtidig langt større.

Gribes processen rigtigt an, og hvis de nye muligheder, der åbner sig ved at gå i clouden, udnyttes fuldt ud, vil virksomheder i processen kunne skabe nye rammer og præmisser for governance, compliance og budgetstyring, så bedre kontrol og mere sikkerhed bliver kombineret med og driver øget agilitet, værdiskabelse og innovation.

I clouden er disse nemlig ikke hinandens modsætninger, men gensidigt fremmende.

Sikkerhed & Risiko

.....

One should only use the Cloud for non-critical services.

Der er noget trygt og godt ved at vide, hvor ens data og IT-hardware befinder sig. På egne servere i et aflukke i kælderen eller bag store jerndøre i et datawarehouse, hvor et antal dedikerede servere kun håndterer én kundes data. Datawarehouses hvor de fysiske faciliteter er sikret imod alt fra stormflod og strømsvigt til indbrud og ildebrand. Det er straks mere betænkeligt i clouden. Hvor befinder serverne sig, hvem deler man dem med, og hvordan kan man være sikker på, at der ikke bliver tabt noget, når det hele tilsyneladende flyder frit rundt mellem servere fordelt på hele kloden?

Så hellere – bogstaveligt talt – blive nede på jorden, hvor der er faste og forståelige rammer.

Men reelt er dette en både dyr og dårlig løsning. Særligt efterhånden som både nationale og internationale myndigheder stiller stadigt større krav til compliance. Ikke længere blot for virksomheder, der håndterer meget følsomme persondata som medicinalindustrien eller den finansielle branche. Med indførslen af GDPR i EU er tæt og dokumenterbar kontrol med både håndteringsprocesser og de fysiske rammer, inden for hvilke data og services kører og opbevares, blevet et ufravigeligt krav for alle virksomheder. Et krav, som for mange er en stor og bekostelig opgave at honorere til fulde.

Med mindre de vælger at gå i clouden.

Skyhøj Sikkerhed

Blandt udbydere af IaaS og PaaS er AWS anerkendt som havende et af de absolut højeste niveauer af sikkerhed. Og de giver deres kunder de bedste redskaber til at opnå det samme. Det sidste vender vi tilbage til. Der er nemlig en ansvarsfordeling, det er nødvendigt at være opmærksom på. For nu fokuserer vi på den del af sikkerheden, hvor AWS har det fulde ansvar, og tilbyder det højeste sikkerhedsniveau, det er muligt at få.

AWS's fulde sikkerhedsansvar ligger under den såkaldte hypervisorlinje.

.....



Her ligger infrastruktur, hardware, de fysiske faciliteter og netværk. Alt der ligger under hypervisorlinjen bliver flere gange årligt kontrolleret og dokumenteret af tredje part, således at brugere af AWS kan anvende det som del af deres dokumentation, der viser, at de er compliant, og så de kan opnå den nødvendige certificering, der måtte gælde for dem. Det er compliance af blandt andet ISO 27001, GDPR, EU-US Privacy Shield, HIPAA og HMDA.

Det er et niveau af sikkerhedscertificering, kun de færreste vil have adgang til eller mulighed for at opnå inden for egen budgetramme. Med AWS er dette til rådighed for alle uanset deres forbrug eller antal konti.

Det er dog stadig 'kun' under hypervisorlinjen. Over denne linje – der hvor de forskellige services og applikationerne kører og bliver benyttet, ligger ansvaret for at have de rette sikkerhedskonfigurationer hos brugerne. Men dette bør langt fra betragtes som et problem, og det er desuden vigtigt at pointere, at en 'sikker' plads på landjorden heller ikke på dette punkt nødvendigvis er garant for sikkerheden.

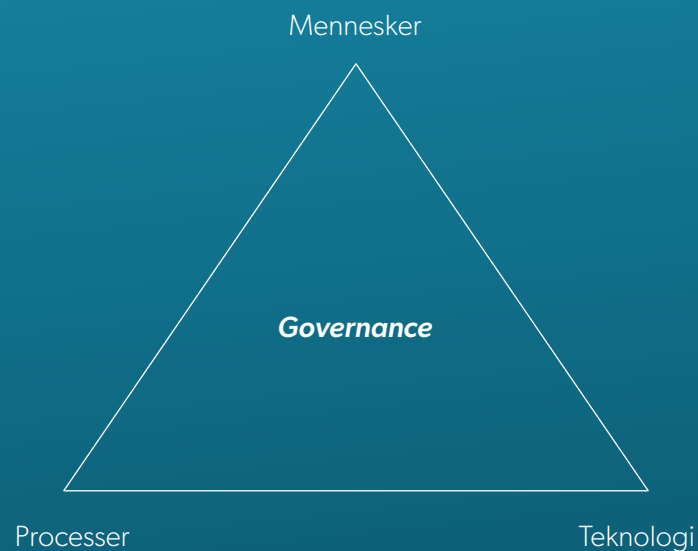
Pointen er, at det skal gøres.

Erhvervsstyrelsen estimerer, at omkring en fjerdedel af danske virksomheder ikke har det fornødne digitale sikkerhedsberedskab til at modstå angreb som phishing og ransomware. DI peger på digitale angreb som en af dansk erhvervslivs største udfordringer i fremtiden.

I en kampagne fra netop Erhvervsstyrelsen afslører virksomheden Bahne, at hackere fik adgang til kundernes kortinformationer, og de måtte lukke deres webshop i flere måneder og opbygge en ny på en anden platform.

IT-governance er død, længe leve governance

Inden vi går videre til den konkrete digitale proces, er det vigtigt at understrege, at vejen til at opnå den bedste og kritisk nødvendige sikkerhedshåndtering begynder over det tekniske niveau. Digitaliseringen er et faktum, alle forretningsgange har en digital komponent, og fuld digital transformation forudsætter en indledende erkendelse af, at IT-sikkerhed skal behandles med en lige vægtning af de tre delmængder: Mennesker, processer og teknologi. Og definitionen af politikker skal foregå på ledelsesniveau med repræsentation af alle dele af forretningen. Disse politikker skal herefter benyttes til beskrivelse af processer og kontroller samt de templates, der definerer design af infrastruktur og konfiguration af alle knyttede services og applikationer.



Sikkerhed i Cloudmigrationens Fire Faser

Når migration til cloud reelt set ikke bør ses som en trussel imod sikkerheden, men snarere en styrkelse, ligger en del af forklaringen allerede før selve flytningen.



1. Analyse

En server eller service i den eksisterende legacy udvælges og en gennemgribende analyse og stresstest af dens sikkerhed gennemføres. Erfaringsmæssigt afsløres der ved denne lejlighed mange kritiske svagheder og huller, der gør det eksisterende meget sårbart for angreb og læk. På baggrund af analysen kan rekonfigurering af legacy gennemføres. Denne rekonfigurering benyttes til en replikerbar template.



2. Modellering

Anden fase er etablering og modellering af clouden. Med CloudFormation udarbejdes en detaljeret template for alle services og applikationer. Dette inkluderer også tilknytning af nye cloud-native sikkerhedsapplikationer.



3. Del-migration

I tredje fase migreres den udvalgte server eller service. Legacy er gennemtestet og bearbejdet til at opfylde alle sikkerhedskrav. Clouden tilsvarende. Del-migrationen kan igangsættes.



4. Fuld Migration

På baggrund af del-migrationen udarbejdes en PoC og en template for fuld migration til cloud. Denne template vil sammen med templateen i CloudFormation og sikkerhedsrekonfigurering af legacy betyde, at den resterende migration kan automatiseres og dermed gennemføres på en fraktion af den tid, det normalt tager. Samtidig med, at gamle sikkerhedsbrist bliver lukket og fremtidige forebygges.

CASE: Pharmacovigilance, Sikkerhed & Compliance

.....

Pharmacovigilance er den samlede betegnelse for overvågning af lægemidlers sikkerhed. Alle aktører i lægemiddelbranchen er forpligtede til løbende at kontrollere, indsamle og formidle information om deres produkters sikkerhed og eventuelle bivirkninger.

At overholde reglerne for pharmacovigilance er en meget omfattende opgave, men med øget digitalisering og udvikling af software er overholdelsen blevet både bedre og nemmere at administrere.

Dog kan fuld digital understøttelse være en bekostelig affære og administrativt tung at løfte i forhold til compliance. Dertil kommer hyppige skærpelser og ændringer af lovgivningen både nationalt og internationalt.

Dette foranledigede en dansk virksomhed til at lancere en service til aktører i medicinalindustrien. En service, der kuraterede de bedste løsninger fra andre leverandører (best-of-breed) samt virksomhedens egne ét sted.

Virksomheden oplevede dog hurtigt udfordringer med hensyn til manglende agilitet, time-to-market og meget lang onboarding-tid for nye kunder. På kundesiden var krav om investering i infrastruktur og vedligeholdelse af applikationer en voksende byrde både økonomisk og administrativt.

Sammen med KeyCore flyttede virksomheden derfor forretningen til en SaaS-løsning i AWS Cloud.

“Udfordringen var, at clouden og de services, der anvendes, skulle opfylde de meget strenge regulatoriske krav, der stilles medicinalindustrien både i relation til compliance og sikkerhed”

CASE fortsættes på næste side..

Løsning

KeyCore assisterede med etablering af en sikker, robust og skalerbar cloudinfrastruktur i AWS, som er både HIIIPA, GxP og GDPR-compliant, hvilket er license-to-operate for virksomheden.

Valget af AWS hang nøje sammen med det meget høje complianceniveau. Med AWS var virksomheden sikret, at alt under hypervisorlinjen til fulde levede op til det strenge compliance-regime alle life-science aktører skal efterkomme internationalt.

Løsningen er designet til at sikre maksimal sikkerhed og adskillelse af de enkelte slutkunder, uden at dette øger management overhead for virksomheden. Dette gælder både allerede etablerede industrispecifikke standartapplikationer samt virksomhedens egenudviklede applikationer.

Løsningen gør det muligt for virksomhedens kunder at anvende alle produkter som en SaaS-løsning. Hvilket betyder, at de kan anvende alle relevante applikationer uden kostbare investeringer i infrastruktur.

KeyCore assisterede desuden med udarbejdelse af templates for en skalerbar infrastruktur, der sikrer en nem og effektiv onboarding af nye kunder i et replikerbart set-up, som overholder de regulatoriske krav for life-science.

Tilsvarende er CI/CD pipelines via templates optimeret til hurtig og effektiv eksekvering med nøje beskrevne politikker og proces for fuld compliance.

“I sammenligning med da kunder tidligere skulle benytte sig af en on-premis-implementering af applikationer, betød transformationen til cloud, at onboardingtiden gik fra måneder til timer.”

CASE fortsættes på næste side..

Anvendt AWS-teknologi:



Multi Account Organizational policies



IAM / Federation



VPC with advanced Peering



CloudFormation



Managed Active Directory



Advanced Windows Management



RDS / Oracle



AutoScaling



System Manager (SSM)



EC2 Automation



LoadBalancing

Agilitet & Innovation

.....

“Manglende udvikling er afvikling.”

Det er den brutale virkelighed, virksomheder opererer i. Dertil kommer, at intet kan tænkes uden at indtænke den digitale dimension.

(næsten) Paradigmeskift til DevOps

Tiden, hvor IT kunne udvikle og implementere på kvartals- endsige månedlig basis er forbi. Ideelt set. DevOps-tilgangen er stadig et stykke fra at være standard. Hvilket ikke mindst skyldes opretholdelsen af traditionel enterprise-tænkning. Man har muligvis på nogle områder grebet SaaS-mulighederne, men der er en iboende inerti forhold til at gå hele vejen til en CI/CD/CD (Continuous Integration/ Continuous Delivery/ Continuous Deployment) arbejdsproces.

Konsekvensen er flaskehalse, manglende innovation og agilitet. Både til at følge med de skiftende behov, løse problemer, udvikle og -vide forretningspotentialer og generelt øge værdiskabelsen.

Dette hænger i høj grad sammen med et ønske om – eller opfattet behov for – central kontrol og godkendelse, og reservationerne i forhold til at købe fuldt ind på en smidig DevOps-tilgang er således de samme, som når det kommer til at kunne opretholde sikkerhed ved migration til cloud.

Og ligesom reservationerne vedr. sikkerhed, således også paradokset:

Migration til cloud vil nemlig åbne op for at udnytte det fulde potential ved DevOps og gøre det med et niveau af kontrol, der aldrig vil kunne matches i en klassisk tilgang til udviklingsprocessen.

Fail fast. Don't Break Anything

Nye idéer og løsninger skal naturligvis underkastes grundige tests. For effektivitet, robusthed, fejl, mangler og endeligt mulige gevinster for virksomheden. Det er ikke noget, man kan tænke sig til eller bygge på antagelser. Den optimale løsning og et validt beslutningsgrundlag kræver med andre ord en PoC, der tager udgangspunkt i den reelle eksisterende infrastruktur.

Dette er stort set umuligt at tilvejebringe i tilfredsstillende skala i en on-premise eller datawarehouse-løsning.

I et skalerbart cloud-miljø forholder det sig anderledes. Den eksisterende infrastruktur kan replikeres til et isoleret testmiljø, hvor nye løsninger, applikationer og services kan blive prøvet op imod det kendte. I dette "beskyttede værksted" har udviklere med andre ord mulighed for at arbejde med alle tænkelige scenarier, køre stresstests i fuld skala og fejle hurtigt uden at ødelægge noget.

Når denne udviklings- og testproces gennemføres i et cloud-miljø som AWS, kan den færdige PoC bruges til udarbejdelsen af en detaljeret template for en automatiseret implementering af den valgte løsning i den eksisterende infrastruktur, hvilket ikke alene sikrer imod risikoen for fejl med en manuel håndtering, men samtidig at den kan gennemføres hurtigt og effektivt.

CASE: PoC banede vejen til AI, ML og massive besparelser

.....

For en af Skandinaviens største mediekoncerner udgør videresalg og genbrug af billedmateriale en ikke uvæsentlig del af forretningen.

KeyCores kunde havde ved projektstart mere end 18.000.000 billedfiler. Voksende med 800.000 om året. For at kunne sælge og genbruge disse billedfiler er det afgørende, at de rette metadata er tilknyttet, med korrekt tagging af motivet – person, sted eller begivenhed – samt yderligere information som fx stemning, aktiviteter og omgivelser.

Det havde hidtil været en manuel opgave, der årligt androg op imod 44 årsværk.

Kunden var allerede fuldt cloudbaseret i AWS og havde derfor adgang til AWS' brede portefølje af tools til optimering af deres håndtering af billedfiler. Imidlertid manglede de et klart billede af hvilke muligheder, der ville være relevante, og hvilken værdi det ville generere. Og mest presserende: Hvor lang og indviklet arbejdsprocessen med at udvikle og teste sig frem til den rette løsning ville blive.

KeyCore anbefalede et nøje tilrettelagt forløb med henblik på en PoC, med klare håndgribelige svar, der spejlede konkrete forretningskritiske udfordringer og problematikker.

Til udarbejdelsen af en PoC blev et testmiljø opsat ved hjælp af AWS CloudFormation, så testmiljøet var en præcis replikation af den eksisterende infrastruktur.

Det isolerede testmiljø gav mulighed for at afprøve og tilpasse forskellige løsninger og tools uden risiko for den fungerende infrastruktur.

Den færdige PoC lå klar efter blot tre uger

Med testmiljøet etableret i AWS CloudFormation lå replikerbar templates for automatiseret implementering af den valgte løsning klar til endelig udrulning.

Med PoC'en fik kunden:

- Hurtigt bevis for forretningsværdi
- Agil adoption af nye teknologier som AI og ML
- Sikker og hurtig implementering af nye services

AWS Recognition

- Person: Ansigtsallokering og -genkendelse
- Setting: Location og aktivitet

Den hidtidige manuelle tagging af billedfiler androg op imod 44 årsværk.

Prisen for det manuelle arbejde var € 3.85 eller ca. 27 kr. pr. billede.

Prisen pr. billede med AWS AI-løsningen er € 0.12 eller lige under én krone.

**“Med en årlig tilføjelse af 800.000 billedfiler
gik omkostningerne med andre ord
fra 21,6 mio. kr. til omkring 680.000 kr.
En potentiel besparelse på næsten 21 mio. kr.”**

2 x Hurtig, Sikker og Effektiv Agilitet og Innovation



1. Automatisering med Templates

Konstant innovation og en organisation med et agilt DevOps-mindset, hvor forretningen driver implementering af nye digitale løsninger eller vice versa.

Et drømmescenarie hentet fra startups, der er født digitale, eller et mareridt, der holder CISOs og CFOs vågne om natten, fordi den løsslupne kreativitet potentielt kan åbne en ladeport i sikkerheden eller sprænge budgetterne og presse kapaciteten til smertegrænsen.

Ikke i cloud.

Der opstår konstant nye behov eller viser sig muligheder, der skal have et hurtigt digitalt modsvare. Det kan være tilpasning af noget eksisterende eller en helt ny applikation, der enten skal bygges fra grunden eller tilpasses fra en standard.

Og det kan hurtigt blive en langstrakt affære. Ikke alene skal den nye applikation naturligvis opfylde de funktionelle krav. Compliance og de seneste opdaterede politikker skal også overholdes. Traditionelt bliver dette sikret gennem intern, central kontrol og endelig godkendelse før launch. Risikoen for flaskehals og deraf afledt forsinkelse er overhængende.

Med AWS er denne pipeline effektiviseret markant. Både hvad angår hastighed og sikkerhed. Med et ubegrænset antal templates for konfigurering, kan alle nye applikationer og services blive underkastet en automatiseret proces: Fra kontrol, tilpasning og godkendelse til endelig launch.

Visse templates for bestemte typer applikationer eller services kan have en specifikation, der kræver en manual godkendelse, men ellers er processen fra behov og idé til endelig brug befriet for alle forsinkende led og de risici for fejl eller forglemmelser, der altid ligger i manuel håndtering.



2. Den Digitale Slikautomat: Landing Zone

Med en AWS-cloudløsning vil alle medarbejdere i princippet have adgang til verdens største udvalg af applikationer og services. Med en AWS-konto er det bare med at plukket ned fra hylderne.

Og dermed ville skrækscenarierne både for mulige sikkerhedsbrist, tab af overblik og løbsk økonomi være en realitet. Samtidig ville det formentlig også give mere forvirring og frugtesløs søgning end kvalificerede valg.

Udfordringen er at give slip på enterprise-løsningens spændetrøje, hvor one size fits all, og finde den rette balance for mellem innovationsfremmende frihed og kontrol.

Til det har AWS udviklet sine såkaldte kataloger. Vi plejer at kalde dem Landing Zones, fordi man her kan lande sikkert og vælge frit.

En Landing Zone kan sammenlignes med slikautomat. Potentielt kan alle brugere eller konti have deres egen automat. Det er kun et spørgsmål om, hvor detaljeret dens konfiguration sættes op. Mest sandsynligt er det dog, at adgangen til de forskellige Landing Zones er fordelt på fx afdeling, ansvar eller jobfunktion.

Hver Landing Zone har et kurateret udvalg af applikationer og services. Standard eller særligt udviklede. Valgt efter relevans for den pågældende konto, fuldt compliant med alle sikkerhedskrav og øvrige politikker.

Ved at tilføje AWS Control Tower har administrator desuden mulighed for et samlet overblik over samtlige Landing Zones på tværs af organisation, afdelinger og teams. Fra AWS Control Tower kan de forskellige templates og konfigurationer administreres og tilpasses, ligesom nye Landing Zones kan oprettes.

CASE: Time-to-market in no time

.....

Hurtig og effektiv kundeservice er afgørende for virksomheders konkurrencedygtighed. Moderne forbrugere stiller høje krav og forventer at blive både modtaget, genkendt og serviceret med udgangspunkt i korrekte og relevante data.

Dette betyder, at evnen til at fremsøge kundeinformation hurtigt er absolut forretningskritisk.

En forsyningsvirksomhed med en stor – og støt voksende – kundebase havde problemer med fremsøgningen af deres kunder i en applikation. Det var klart, at noget skulle ændres. Spørgsmålet var hvad og hvordan:

- Agil adoption af nye teknologier som AI og ML
- Sikker og hurtig implementering af nye services

Udvikling, test og implementering af denne type service bliver typisk betragtet som meget ressource- og tidskrævende. AWS giver imidlertid adgang til agilitet og hastighed, der redefinerer traditionel opfattelse af time-to-market.

Proces

KeyCore assisterede dels virksomheden i analysen af problemets rod, samt orkestrering af en ny løsning, der sikrede den ønskede optimering af den forretningskritiske applikation.

For at have et informeret grundlag at arbejde ud fra, blev et testmiljø, der spejlede det eksisterende miljø, opsat. Dette var ganske simpelt i AWS CloudFormation, hvor infrastruktur nemt og hurtigt kan replikeres.

Testmiljøet blev herefter underkastet en stresstest (SPT) med 25 gange så meget data, som normalt blev håndteret.

Dernæst blev et nyt testmiljø opsat med en væsentlig opskalering af serverkapaciteten.

Dette testmiljø blev ligeledes underkastet en SPT.

Sidste trin var et testmiljø med en kapacitet svarende til det eksisterende, men med Amazon Elasticsearch Service som søgeapplikation. Dette testmiljø blev som de andre underkastet en SPT.

På baggrund af dette havde virksomheden nu en PoC, der tydeligt viste, hvor problemet lå og følgelig, hvilken løsning de skulle gå efter.

Resultatet var ikke til at tage fejl af:

Med testmiljøet etableret i AWS CloudFormation lå replikerbar templates for automatiseret implementering af den valgte løsning klar til endelig udrulning.

- Den nuværende løsning kunne gennemføre cirka 1.500 søgninger i timen
- En løsning med en øget serverkapacitet kunne gennemføre cirka 5.000 søgninger i timen
- Løsningen med Amazon Elasticsearch Service kunne gennemføre mere end 10.000 søgninger i timen. Vel at mærke, uden at øge kapaciteten.

På baggrund af PoC'en kunne virksomheden træffe et informeret valg og undgå at spille unødige ressourcer på øget kapacitet, der ikke ville give den ønskede optimering

Samtidig lå template for implementering af Amazon Elasticsearch Service i deres eksisterende infrastruktur klar i AWS CloudFormation.

Time-to-market

Samlet havde opsætning af testmiljøer og SPT taget én arbejdsdag. Med replikerbar templates i AWS kunne overgangen til Amazon Elasticsearch Service som søgefunktion gennemføres fuldt automatiseret og derfor både hurtigt, sikkert og effektivt, hvilket sikrede, at virksomhedens kunder hurtigt oplevede en markant bedre service.

Skalérbarhed & Ressourceudnyttelse

Ved de indledende drøftelser om transformation fra on-premise eller warehouse til cloud er spørgsmålene og bekymringerne for sikkerhed og compliance, samt om en mindre central kontrol med, hvilke digitale eventyr medarbejdere og afdelinger kaster sig ud i, vil sende virksomheden ud på uproduktive sidespor, altså tilbagevendende faktorer, der bremser processen.

Som gennemgået i de foregående kapitler hviler disse bekymringer heldigvis i vid udstrækning på misforståelser.

Det samme gælder den næste bremsende faktor, der næsten uafslædt dukker op.

Elastik i Metermål

Uanset om der er tale om on-premise eller datawarehouse, er de økonomiske rammer omtrent de samme. Det er en fast driftsomkostning med veldefinerede grænser for kapaciteten. Der er den plads og den kraft, man har aftalt, og det ændrer sig ikke, uanset i hvor høj grad man benytter det eller måtte have brug for mere. Lyset er – så at sige – altid tændt, og hvis man vil have flere lamper, må man lave en ny aftale for den næste afregningsperiode eller indkøbe nogle flere.

I henseende til sikkerhed er der med andre ord stor budgetmæssig tryghed ved en on-premis eller warehouse-løsning, da det antyder en stor grad af kontrol og forudsigelighed.

Set fra et forudsigelighedsperspektiv indikerer begreber som skalerbarhed modsat en større usikkerhed. Og den budgetansvarlige kunne godt støde sig på AWS' EC2, der er en forkortelse for Amazon Elastic Compute Cloud:

- Det kræver – som Storm P. skrev – ærlighed at sælge elastik i metermål, og hvis der bare kan skaleres op efter forgodtbefindende, kan budgetelastikken blive strakt mere, end rammerne kan holde til.

Det kan virke besnærende med faste og forudsigelige rammer for kapaciteten. Hvis det da ikke lige var fordi, den virkelighed, denne kapacitet skal fungere i, hverken er fast eller forudsigelig, og at forkert dimensionering – både op, ned og i anvendelse – kan have meget alvorlige negative konsekvenser.

De 3 Elasticiteter

Op

Mulighed for opskalering er ofte det, der bliver peget på som den primære årsag til at flytte til et skalerbart cloud-miljø. Med god grund. Helt lavpraktisk er det en forudsætning for, at virksomheden kan understøtte vækst. Det være sig i medarbejdere, afdelinger, services eller applikationer. Hurtig onboarding og implementering forudsætter hurtig opskalering.

Men evne til håndtering af spikes bliver tilsvarende stadig mere kritisk. Pludselig markant stigning i fx webtrafik eller akut behov for håndtering af store workloads er vilkår, alle virksomheder i dag bør være forberedt på.

Manglende agilitet til at øge kapaciteten - elasticitet – kan i den milde ende medføre forlængelse af svartider, og i den alvorlige; sammenbrud pga. overbelastning.

Uanset, har manglende evne til at sikre den nødvendige kapacitet forretningsskadelige konsekvenser.

Ned

Lamperne er altid tændt. Det var billedet på en on-premise eller warehouse-løsning. Uanset om alle medarbejderne er taget på sommerferie, eller det er den travleste dag på ugen, kører man med uændret blus. Efter en tidligere oplevelse med spikes har man måske endda besluttet at tilkøbe mere kapacitet, så man er klar. Hvis nu.

Set fra det perspektiv er en on-premise eller warehouse-løsning i forhold til en skalerbar cloud som AWS den dyreste – og indlæst i en klimadagsorden – den mest belastende og ubæredygtige vej.

I anvendelse

Med en on-premise eller warehouse-løsning, hvor der er en fikseret ramme for kapaciteten og en tilsvarende faste rammebetingelser for de forskellige applikationer og services, er mulighederne for agilitet og samtidig optimal udnyttelse af kapacitet meget begrænsede.

Med brug af AWS' tools til analyse samt budget- og ressourcestyring bliver der åbnet for nogle helt nye muligheder.

Sikker Økonomi i Clouden

På et splitsekund

Det første, der er væsentligt at fremhæve i forhold til ressourceforbrug, når det kommer til cloud vs. on-premise eller datawarehouse, er, at i en cloud som AWS betaler man kun for det, man bruger.

Helt ned til et splitsekund.

Det betyder to ting: For det første åbner det for et meget detaljeret indblik i, hvor og hvordan kapacitet og ressourcer bliver brugt, og for det andet, at der er meget at hente, hvis forbruget kontinuerligt bliver trimmet og optimeret. Selv med et setup, der tillader meget store periodiske spikes i kapaciteten, kan en cloud, der er orkestreret og håndteret optimalt være langt billigere end en on-premise-løsning.

Det hele kan koges ned til at benytte de rette tools og have veldefinerede politikker.

AWS tilbyder en lang række muligheder for kontrol, analyse og skalering af kapacitet og ressourcer. Hvilke, der er bedst og mest relevante, kommer naturligvis an på konkrete behov, men vi har valgt at fremhæve nogle, der næsten uanset hvad vil give den ønskede kombination af overblik, kontrol og agilitet gennem skalerbarhed

Indblik & Overblik

Det hele begynder med at sætte en lap på.

Alle ressourcer og services i clouden kan tilføjes et tag. Det kan ske på to måder. Enten AWS Generated Tags eller User-Defined Tags. Disse tags bruges til at kategorisere, organisere, analysere og kontrollere de forskellige ressourcer og services. Der er ingen begrænsninger på, hvor mange tags en given ressource eller service kan have og særligt med de brugerdefinerede tags giver det mulighed for generering af mange værdifulde indsigter og styringsredskaber.

I henseende til det økonomiske kan administrator med AWS' Cost Allocation Tagging og Cost Explorer via både de autogenererede og brugerdefinerede tags trække filtreringer lavet på tværs af organisationen, hvor man ser på forbruget fra forskellige services. Det kunne være med funktions-tags som 'webshop', 'kommunikation' eller 'regnskab'. Eller mere brugerdefinerede som ejer, afdeling eller slutbruger. Helt ned til den sidste krone eller det sidste sekund.

Med taggingen kan individuelle budgetrammer på tværs af organisation og funktionaliteter defineres. Dette er en oplagt lejlighed til at se på, hvad der betragtes som forretningskritisk.

Hvilket leder videre til næste tool.

Kontrol & Skalering

Ikke for lidt. Ikke for meget. Men heller ikke elastik i metermål.

Applikationer og services skal være tilgængelige og kunne håndtere spidsbelastninger. Men lyset skal ikke stå og brænde, når der ikke er brug for det.

Derfor har AWS udviklet deres tool Auto Scaling, som giver adgang til at skalere kapaciteten op og ned efter behov og efter predefinerede grænseværdier.

Det kan ske på tre måder:



Planlagt

Vil marketing kører en større kampagne med forventet massiv forøgelse af trafikken til webshoppen? Ved kundeservice, at der kommer tryk på kedlerne ved kvartalsafslutning?

Mange spidsbelastninger kan forudses. Med Auto Scaling kan en manuelt godkendt automatisk op- og efterfølgende nedskalering i et afgrænset tidsrum sikre, at kapaciteten er på plads, når og hvor der er brug for den.



Forudset

Auto Scalings ML analyserer mønstre og tilpasser løbende forudsigelser om kommende belastning. De genererede algoritmer gør automatisk skalering enklere at konfigurere.

ML-analyseværktøjet giver desuden værdifulde indsigter i applikationer og services' "sundhedstilstand" og benyttelse. Med indsigterne kan uvirksomme eller fejlbehæftede applikationer og services lukkes ned, og kapaciteten allokeres til andre eller nye.



Dynamisk

Sæt kapacitetsmål for applikationer og services og lad herefter Auto Scaling sørge for at kapaciteten automatisk bliver skaleret op og ned efter behov.

Ønsker du mere viden om AWS, sikkerhed, digital transformation og cloudmigration?

.....

KeyCore er certificeret AWS Advanced Consulting Partner og AWS Public Sector Partner.

Vores konsulenter er højt specialiserede eksperter, der både rådgiver og leverer digitale løsninger, der understøtter fremtidig værdiskabelse, forretningsudvikling og naturligvis det højeste digitale sikkerhedsniveau.

“Kontakt os for en uforpligtende samtale om jeres behov og vores bud på den bedste løsning.”

.....

Ring til os på

29 83 86 70



KEYCORE

Cloud Specialister