Microsoft Azure

intel

Moderniser dine forretningskritiske systemer og applikationer med en cloud-løsning

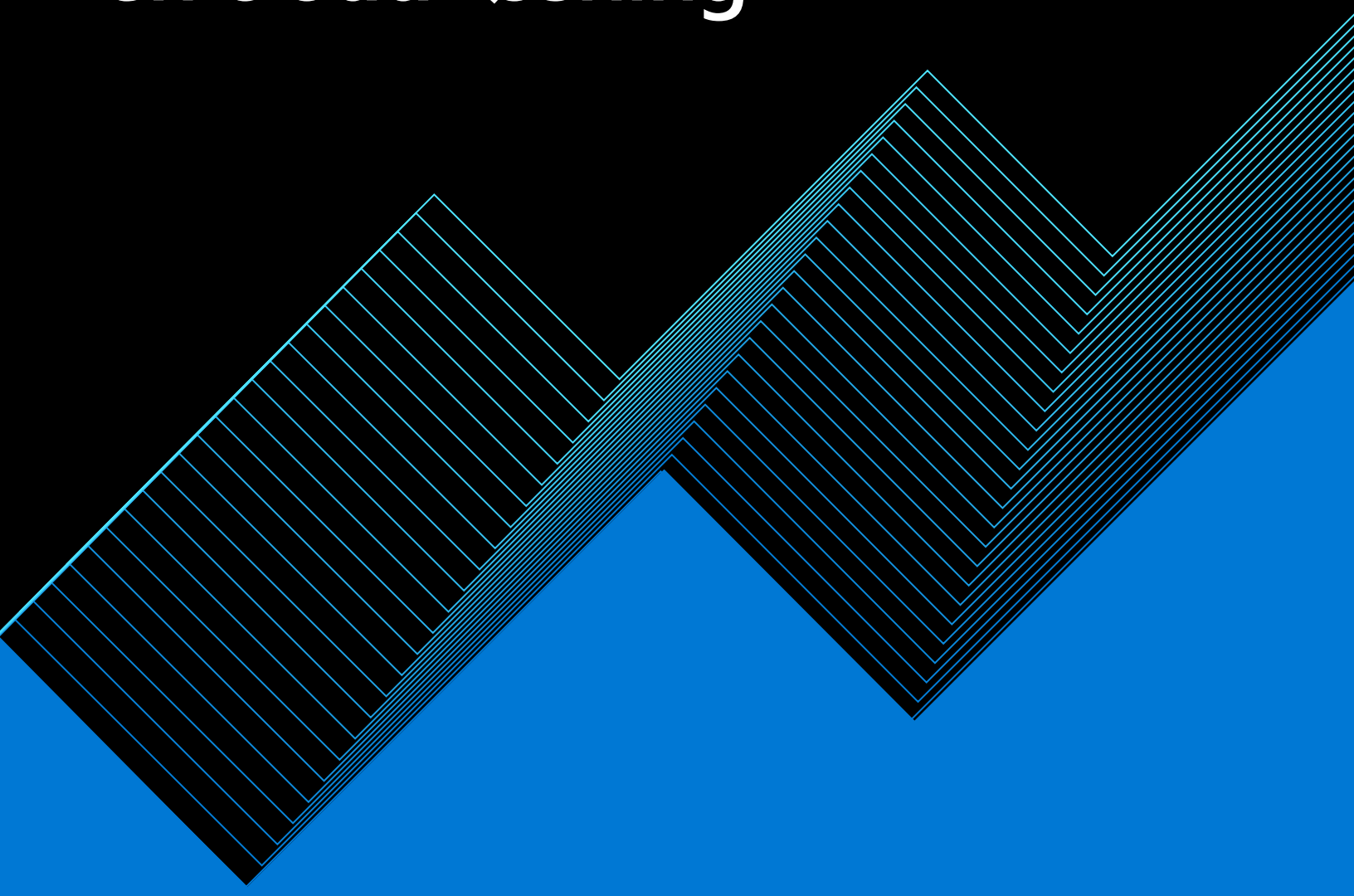


Table of contents

01

Introduktion

Udtrykket "virksomhedsmodernisering" er blevet et buzzword i diskussioner om virksomhedsplanlægning, og dets betydning er ofte udtyndet og tvetydig. Virksomhedsmodernisering refererer imidlertid blot til modernisering af de applikationer og systemer, som virksomheder er afhængige af i den daglige drift. De vigtigste af disse betragtes som "missionskritiske" eller "forretningskritiske" systemer. Definitionerne kan variere fra virksomhed til virksomhed, men behovet for, at disse systemer er pålidelige, hurtige, tilgængelige og sikre, er universelt.

Hver organisation har sin egen definition og sine egne parametre for, hvad der er forretningskritisk. I forbindelse med denne e-bog anvender vi den herskende branchedefinition, dvs. at forretningskritiske systemer og applikationer normalt er dem, der understøtter en virksomheds vigtigste forretningsprocesser. Dette er ofte de systemer, der, hvis de forstyrres, kan påvirke indtægter, omdømme og kundeoplevelser negativt. Derfor kræver forretningskritiske systemer ofte de højeste serviceaftaler for en bestemt organisation.

Mange virksomheder har flyttet eller planlægger at flytte forretningskritiske workloads til public cloud-infrastruktur, og de intensiverer fokus på overgangen til en cloud-løsning ud over indledende proof of concept, backup, udvikling og test af workloads. Der opstår spørgsmål om, hvordan man definerer forskellige grader af, hvor forretningskritisk noget er. Det er nødvendigt at opdage, dokumentere og i sidste ende styre kompromiserne mellem tilgængelighed og forretningskontinuitet, robusthed, ydeevne, omkostninger og kompleksitet. Organisationer i regulerede brancher og i den offentlige sektor skal også konsekvent overveje yderligere faktorer.

Vores samtaler med it-chefer bekræfter, at det kan være temmelig udfordrende at administrere forretningskritisk infrastruktur on-premises. Faktisk fortæller organisationer, der har migreret deres forretningskritiske systemer til en cloud-løsning, at de har øget deres evne til at opfylde krav til sikkerhed og overholdelse af regler og standarder. De nævner hurtigere implementering af infrastruktur og større skalerbarhed i kombination med større driftsmæssig fleksibilitet. Ikke desto mindre har kunderne brug for gennemprøvede og pålidelige migreringsmetoder. Microsoft og deres partnere i regioner overalt i verden har ført an og understøttet tusindvis af vellykkede migreringer samt konsolideringer og ophør af datacentre i det seneste årti. Vores erfaring med forretningskritiske workloads giver os mulighed for at udarbejde og finjustere en migreringsmetode, der er skræddersyet til de specifikke behov og prioriteter i din organisation.

Den første halvdel af denne e-bog viser, hvordan man afklarer, kvantificerer og skelner mellem forretningskritiske systemer. Den anden halvdel dykker dybere ned i trinnene og de teknologiske overvejelser i et eksempelscenarie med fokus på SAP-applikationer. Det giver vigtig viden og indsigt, så du kan forstå kravene, risiciene og alternative tilgange til at flytte dine forretningskritiske systemer til skyen.

02

Definition af “virksomhedskritisk”

Kunderne evaluerer typisk flere kriterier for at definere, hvor forretningskritisk en applikation eller et system er. Følgende er de mest almindelige kriterier, som vores kunder bruger:

1. **Serviceaftaler (SLA'er) eller andre tilgængelighedsmål:** Forretningskritiske systemer og applikationer er normalt dem, der har den højeste SLA for en bestemt organisation, hvilket normalt udtrykkes som en procentdel. En SLA på 99,99 procent har en akkumuleret nedetid på 4,32 minutter pr. måned eller 52,56 minutter om året.

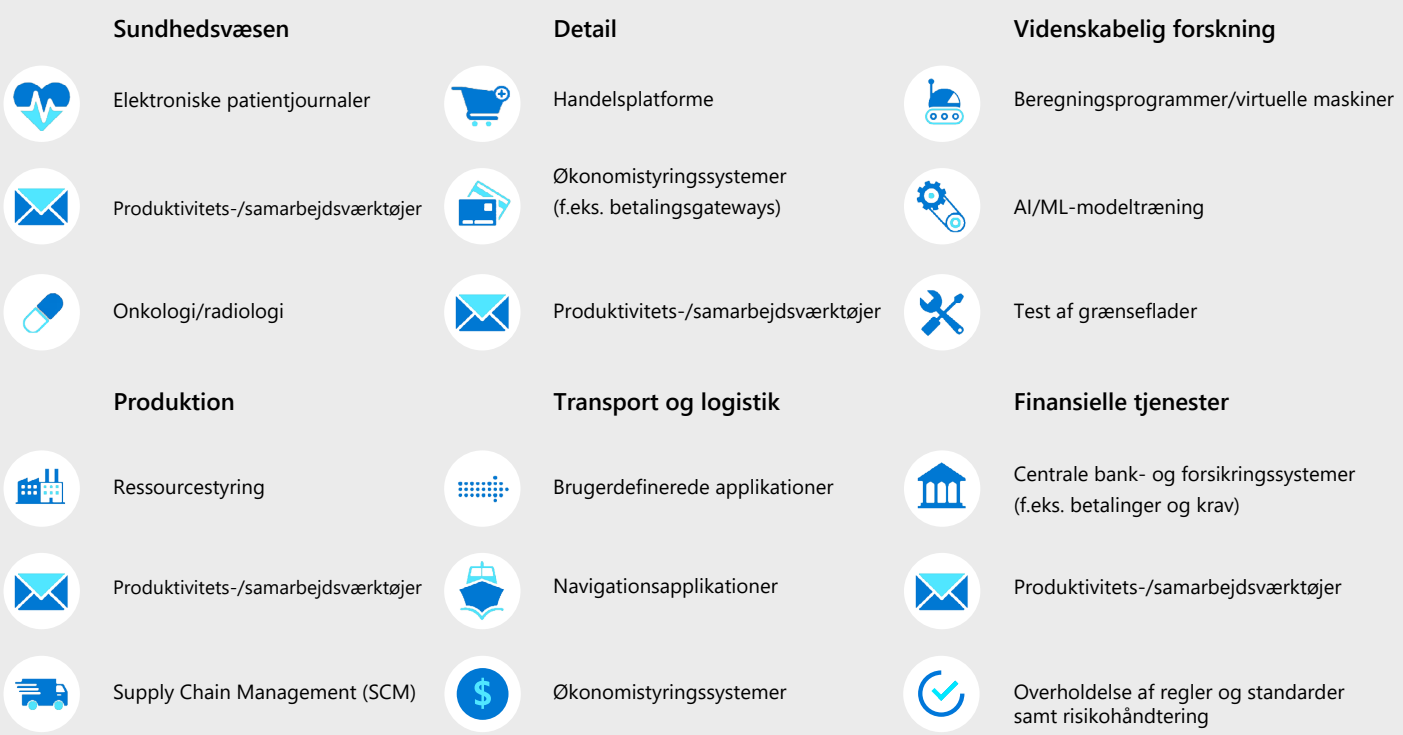
2. **Branchespecifikke mål:** Den type systemer, der oftest klassificeres som forretningskritiske, er de kunderettede applikationer, som en organisations kunder er afhængige af for at drive forretning og foretage transaktioner. Derudover kan vi tilføje kontor- og administrationssystemer med ansvar for økonomistyring, datastyring, risikostyring og overholdelse af regler og standarder (GRC) samt systemer til produktivitet og samarbejde (herunder mail- og kommunikationsværktøjer).

3. **Tab af omdømme eller tillid:** De vigtigste virksomhedssystemer er dem ,der udgør kernen i en virksomheds kritiske processer – dem, der resulterer i de største omkostninger, når de er nede eller går tabt, og som ville have den største indvirkning på omdømmet, hvis der sker et brud på sikkerheden.

Når it-fagfolk planlægger at flytte deres applikationer til skyen, antager de fleste, at cloud-platformen automatisk håndterer størstedelen af løsningens pålidelighed og funktioner til disaster recovery. Men cloud-modellen er afhængig af, at der er et fælles ansvar mellem cloud-udbyderen og kunden. Derfor er der visse SLA'er, som leveres af leverandøren for at understøtte din applikation, men ansvaret for applikationens robusthed ligger hos applikationsejeren.

Definitionen af "forretningskritisk" kan variere, men udtrykket refererer blot til et system, der er kernen i en virksomhed, og som kræver de nødvendige sikkerheds- og designovervejelser for at sikre, at det forbliver robust, skalerbart, vedligeholdelsesvenligt og til en vis grad "fremtidssikret".

Diagrammet herunder illustrerer et par eksempler på typiske forretningskritiske workloads efter branche:



Baseret på: Onlineundersøgelse med 412 beslutningstagere i globale virksomheder og seks dybdegående telefoninterviews med it-topledere
Kilde: The Move Is On: Modernize Mission-Critical Systems with Cloud, en undersøgelse foretaget af Forrester Consulting på vegne af Microsoft, marts 2020

Figur 1. *Forretningskritiske applikationer efter branche*

Identifikation af virksomhedskritiske applikationer

I vores kundesamtaler bruger vi hos Microsoft følgende struktur til at registrere og prioritere applikationer. Den er beregnet til at tilpasse forretningen og it-løsningen til hinanden og at afdække den applikationskontekst, der er vigtig for planlægningen af rejsen mod implementering af cloud-løsningen.

Strukturen er beregnet til at blive brugt fra top til bund. Først gennemgår vi applikationer efter type og skelne mellem indbyggede Microsoft-applikationer (f.eks. .NET-applikationer), kommercielle standardapplikationer og andre løsninger og platforme. Dernæst identificerer vi, hvor forretningskritiske de gennemgåede applikationer er – hvilket er hovedemnet i dette whitepaper. Til sidst, men bestemt ikke mindre vigtigt, foretager vi en indledende vurdering af risiko og kompleksitet.

Figur 2. *Struktur for vurdering af din portefølje*

03

Cloud-migrering: Udfordringer og fordele

Cloud computing tilbyder elasticitet, multikanaludvidelse, hurtigere implementeringer og administration af infrastruktur gennem infrastruktur som kode, hvilket giver lethed og dokumenterede økonomiske fordele. På dette tidspunkt inkluderes alle workloads, herunder ældre applikationer. Mange organisationer anvender en "cloud-fokuseret" tilgang og tager samtidig hensyn til det stigende udvalg af hybrid-, multicloud- og edge-løsninger. Bekymringen om mulige fejl kan dog vare ved.

Nogle gange er kunderne bekymrede over, at cloud-tjenesteudbydere styrer infrastrukturlaget, mens cloud-forbrugerne ikke har kontrol over de fysiske ressourcer. Derudover forbliver overholdelse af regler og standarder og potentielle sikkerhedssårbarheder med de nye cloud-tjenester bekymringer for alle kunder, der er interesserede i at flytte deres forretningskritiske og datafølsomme workloads til skyen.

Deling af et netværk under flere lejere (dvs. deling af workloads med andre lejere), datatab og lækage af data, fælles fysisk placering, servicekvalitet og ressourcekvoter er nogle af de primære bekymringer i forbindelse med migreringen af forretningskritiske applikationer til skyen.

Andre udfordringer i løbet af cloud-migreringsfasen omfatter flytning af meget store mængder data og hosting i flere regioner. I det følgende beskrives de almindelige risici, der er nævnt ovenfor, og metoder til at afhjælpe dem.

Finjusterede kontroller af sikkerhed og overholdelse

Trusselsteknikker ændrer sig konstant. Cyberangreb viser sig i nye former, herunder brugen af botnets til at styre netværk, cloud-drevne angrebstaktikker og anvendelse af ransomware som en tjeneste. En applikation skal være bygget sikkert i standardarkitekturen med en sikkerhedsmodel, der er effektiv til aktuelle og fremtidige behov, såsom mobile arbejdsstyrker, enheder, applikationer og dataadgang. Anvendelse af en Microsoft-sikkerhedsstruktur som Nul tillid-modellen (dvs. hav aldrig tillid, men kontroller altid), kan være et effektivt værktøj til håndtering af

eventuelle trusler. Grundprincipperne bag Nul tillid er ressourcepolitikker for overholdelse af regler og standarder, managementgrupper, multifaktorgodkendelse, brug af minimumsrettigheder til adgang, just-in-time-adgang, antagelse af sikkerhedsbrud samt reduktion af spændvidden for at minimere effekten. Azure-managementgrupper og -politikinitiativer indeholder detaljerede kontroller for overholdelse af regler og standarder til rapportering eller beskyttelse af adgangen til Azure-abonnementer. Endelig kan Active Directory-integrationer, kryptering (med Microsoft- eller kunde-administrerede nøgler), aktivering af Private Link samt funktioner til replikering i flere regioner reducere risikoen for platformen på en nem og praktisk måde.

Multicloud

Vi definerer her "multicloud" som den formålsbaserede brug af PaaS (Platform as a Service), IaaS (Infrastructure as a Service) og SaaS (Software as a Service) fra flere cloud-udbydere. Disse tjenester er typisk en kombination af offentlige, edge- og hybrid cloud-implementeringsmodeller. Der viser sig bestemt at være nogle kompromiser ved brug af denne tilgang, og den bør derfor evalueres nøje. På den ene side kan mange drage fordel af fleksibiliteten og markedets bedste funktioner i en multicloud-løsning. På den anden side udgør den øgede kompleksitet og de øgede omkostninger på grund af behovet for flere kvalifikationer til implementering og support, såsom at opretholde flere automatiseringsstrukturer på tværs af platforme, klare ulemper. Dette kan gøre dine DevOps-funktioner endnu mere komplicerede. Overvej dine specifikke forretningskritiske anvendelsesformål, og evaluer kompleksitet i forhold til fleksibilitet i forbindelse med management og styring, integration, dataspredning og kvalifikationskrav.

Udnyttelse af cloud-udbyderens skalering og elasticitet

Til forretningskritiske applikationer forventer organisationer, at økosystemet giver kontrol, synlighed, elasticitet og skalerbarhed. Azure som cloud-udbyder leverer værktøjssæt som overvågning på infrastruktur- eller applikationsniveau, beskyttelse mod identitetstrusler og tjenester som skalasæt for virtuelle maskiner, så du hurtigt kan implementere udskalering og let tilgængelige applikationer, storage-konti og apptjenester. Webhooks, funktioner og ønskede tjenestetyper til tilstandskonfiguration kan give hurtige reaktionstider og dermed opnå elasticitet eller skalerbarhed for cloud-løsningen. Minimal modernisering af applikationerne på Azure (f.eks. brug af Azure-filshare i stedet for de traditionelle on-premises-filservere) er en anden måde at opnå skalerbarhed på.

Tilgængelighed af cloud-ressourcer fra udbyderen i forhold til kritiske mål

Hvis der opstår en regional fejl, er det en af de mest kritiske opgaver at sikre tilstrækkelige cloud-ressourcer. Identificering og kortlægning af SLA'en for PaaS, IaaS, domænenavnesystem, hemmeligt lager og databasetjenester er vigtige komponenter i et disaster recovery-scenarie. Et forretningskritisk applikationsdesign skal håndtere disse udfordringer og sørge for den nødvendige afhjælpning af risici. Hvis de planlægges korrekt, giver disaster recovery-tests med den applikation, der hostes i skyen, nem og praktisk adgang til produktions-failover ved hjælp af tjenester som Azure Site Recovery til IaaS, indbyggede replikeringssystemer til PaaS og storagereplikering til den parrede region. Alternativt kan du bruge cloud-automatisering og DevOps-værktøjer og -processer til automatisk gendannelse af Azure-infrastrukturen. På denne måde kan applikationen foretage failover til den nyligt lancerede Azure-infrastrukturtjeneste. Du kan også bruge reservationer af on-demand-kapacitet til at dække og fastlægge dine behov for databehandlingskapacitet, når du skalerer op og ned på din forretningskritiske infrastruktur eller udfører softwareopdateringer og -implementeringer.

Forudsigelse af adfærd

Servicekvaliteten for applikationer, der er implementeret i skyen, kan være anderledes end for applikationer, der implementeres on-premises, hvor endpoints tilgås ved næste netværkshop. Forudsigelse af adfærd og løbende prognoser kan hjælpe med at undgå fald i applikationens servicekvalitet. Overvej at flette, forbinde, overvåge og forudsige løsninger med cloud-tjenester. Tidlig registrering af fejl i applikationers ydeevne eller kvalitet kan være nyttige i forhold til beslutningsmatrixen, når applikationskomponenter skal op- eller nedskaleres.

Omkostninger ved at køre kritiske applikationer i skyen

Applikationshosting i skyen kan være dyrt over tid, hvis der ikke er defineret effektive kontroller. Prognoser for år et til fem hjælper med at forstå udgifterne til forbrug af applikationsressourcer.I sådanne scenarier kan evaluering af hostingteknikker, som f.eks. standardimplementering i forhold til at anvende masser af skalasæt eller brug af containere til typer af tjenester, løse omkostningsproblemer ved at anvende modellen med betaling efter forbrug til cloud-løsningen. Reservation af forekomster af databehandlingskapacitet ud fra forventet brug, brug af tredjepartsudbyder i forhold til cloud-udbyder til indbyggede løsninger, brug af varm eller kold infrastruktur til parrede regioner eller styring af ressourceimplementering med en styrepolitik er et par af metoderne til effektivt at kontrollere brug af og udgifter til forretningskritiske applikationer.

04

Forretningskritisk: Nøgleprincipper

Moderne virksomheder kræver en samling af de medarbejdere, processer og teknologier, som skal samarbejde om at levere effektive løsninger og resultater til kunderne. Hvis et forretningssystem skal levere værdi, skal det være pålideligt og så optimalt som muligt, så det er muligt at opnå omkostningsbesparelser og samtidig opnå markant fordel. Azure-cloud-platformen giver et robust fundament, der er bygget på global infrastruktur i verdensklasse. Dette fundament kan udvides med yderligere robusthedsfunktioner ud fra, hvor forretningskritiske dine systemer er.

Dette afsnit indeholder en oversigt. Kontakt Microsoft eller en af vores certificerede partnere, hvis du vil have mere at vide om de emner, der er beskrevet nedenfor. Ud over denne indledende oversigt henvises der til tillægget, især Well-Architected Framework, som dækker disse grundprincipper i flere detaljer.

Følgende er de vigtigste principper, som virksomheder søger i forretningskritiske cloud-platforme:

- Datastyring og virksomhedspolitik
- Robusthed, forretningskontinuitet og disaster recovery
- Ydeevne
- Pålidelighed
- Sikkerhed
- Omkostningsoptimering og driftsmæssig fleksibilitet

Datastyring og virksomhedspolitik

Virksomhedspolitikker fremmer cloud-styring. Vejledningen til styring af Cloud Adoption Framework (CAF) fokuserer på specifikke aspekter af virksomhedspolitikken:

Forretningsmæssige risici: Identifikation og forståelse af virksomhedsrisici.

- Dokumentér lurende forretningsmæssige risici og virksomhedens tolerance over for risici på baggrund af dataklassificering og applikationsvigtighed.

Politik og overholdelse af regler og standarder: Konverter risici til politikerklæringer, der understøtter eventuelle overholdelseskrav.

- Konverter risikobeslutninger til politikerklæringer for at fastlægge grænser for anvendelse af cloud-løsninger.
- Overvej og indarbejd lovmæssige krav.

Processer: Etabler processer til at overvåge overtrædelser og sikre overholdelse af de definerede politikker.

Robusthed, forretningskontinuitet og disaster recovery

Hvis du vil sikre effektiv forretningskontinuitet og disaster recovery, skal din organisation eller virksomhed designe velegnede funktioner på platformsniveau, som applikations-workloads kan bruge til at opfylde deres krav. Specifikt har disse applikations-workloads krav i forbindelse med RTO (recovery time objective) og RPO (recovery point objective). Hvis du vil designe funktioner, der passer til disse workloads, skal du sørge for at opfylde dine krav til disaster recovery (DR).

Kritiske robusthedsfunktioner kan opnås via en række Azure-tjenester, herunder tilgængelighedszoner, tilgængelighedssæt, Azure Traffic Manager, Azure Site Recovery, Azure Backup og Azure Storage.

Ydeevne

Virtuelle maskiners ydeevne: Dine forretningskritiske systemers ydeevne kan direkte påvirke kundetilfredsheden, kundeloyaliteten og i sidste ende din bundlinje. Microsoft fortsætter samarbejdet med teknologileverandører som f.eks. Intel om at integrere deres seneste innovationer i Azure IaaS-teknologien. Derfor kan Azure, blandt andre fordele, levere de løbende forbedringer af infrastrukturens effektivitet, som kunderne forventer af skyen. Azure yder bred support til en række forskellige workloads på Azure IaaS, lige fra Red Hat OpenShift til SQL® Oracle og SAP samt andre systemer. Dette dokument fokuserer på vores viden om at flytte SAP til Azure som indeholder vigtige forretningskritiske workloads.

Hvis du implementerer de nyeste Azure-VM'er kan du forbedre dine applikationers ydeevne, samtidig med at du holder styr på omkostningerne.

De nyeste Intel-baserede Azure Virtual Machines indeholder:

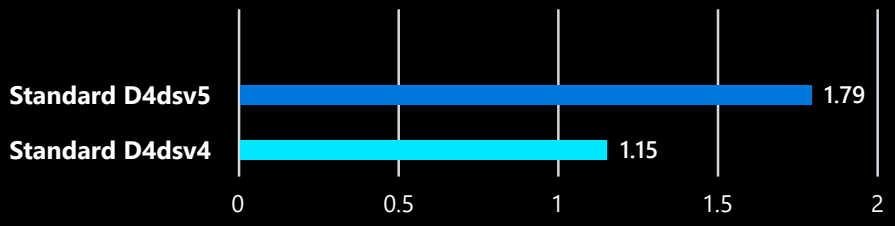
- Nye AVX-512-instruktioner og arkitekturfunktioner paralleliserer eksekveringen af krypteringsfunktioner, hvilket reducerer straffen for at implementere gennemgående datakryptering**, hvilket genererer højere overførselshastighed for krypteringsintensive workloads som f.eks. SSL-webserver.

- Bitnami har i samarbejde med Intel udgivet to afbildninger på Azure Marketplace, der er skræddersyet til 3. generation af skalerbare Intel® Xeon® processorer, som er baseret på Azure Dv5 VM'er, der indeholder Intel-kryptografiske softwarebiblioteker.

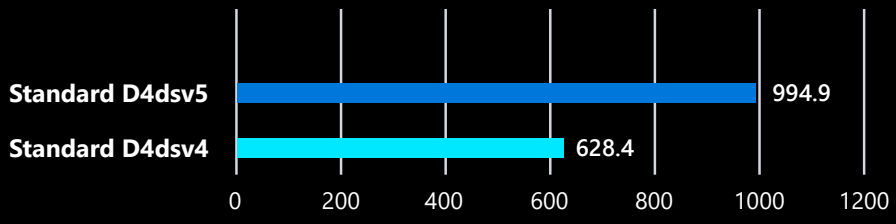
NGNIX: https://azuremarketplace.microsoft.com/marketplace/apps/bitnami.nginx-intel

WordPress: https://azuremarketplace.microsoft.com/marketplace/apps/bitnami.wordpress-intel

Med den indbyggede kryptoacceleration, der leveres af 3. generation af skalerbare Intel® processorer leverede VM'er i Dv5-serien en stigning i overførselsydeevnen på 58 % og en reduceret gennemsnitlig ventetid på 55 % i sammenligning med den foregående generation af Intel-baserede VM'er. Desuden udførte D4dsv5 ca. 55 % flere tråde end D4dsv4.



Figur 3. *Samlet antal trådudførelser (antal millioner) – det samlede antal https-anmodninger, der blev udført i en 30-minutters stresstest*



Figur 4. *Overførselshastighed (antal/s) – samlet antal https-transaktioner pr. sekund*

Ifølge en nylig benchmarkrapport udarbejdet af Principled Technologies har de nye Eds v5-VM'er behandlet SQL Server-workloads betydeligt hurtigere end den tidligere generation af VM'er. Den tid, det tager at fuldføre workloads, kan være op til 1,27 gange hurtigere for virksomheder, der bruger mellemstore VM'er. Dette kan gavne kunderne, så de kan få dataindsigt på kortere tid og dermed hurtigere forbedre deres virksomhed.

- 1,23 gange for virksomheder, der bruger små VM'er med 8 vCPU'er og en database på 30 GB
- 1,27 gange for virksomheder, der bruger mellemstore VM'er med 16 vCPU'er og en database på 100 GB
- 1,23 gange for virksomheder, der bruger store VM'er med 64 vCPU'er og en database på 300 GB

Læs mere om workloads og konfigurationer i: Principled Technology Ice Lake SQL Server Azure

MySQL-databaseanalyse udføres 64 % hurtigere med 3. generation af skalerbare Intel® Xeon® processorer i forhold til før 4. generation.

Se 81 på www.intel.com/3gen-xeon-config. Resultaterne kan variere.

Databasens ydeevne: Graden af hvor forretningskritisk noget er, får ekstra betydning, når man overvejer hastigheder for datainput, output og transaktioner. Et eksempel er applikationer til behandling af onlinetransaktioner, der kræver høje transaktionshastigheder og lav IO-ventetid. Denne type system kræver ikke kun den højeste modstandsdygtighed over for fejl, men også hurtige failovers ved hjælp af flere synkront opdaterede replikaer. Azure SQL Database har et specifikt forretningskritisk lag, der er designet til workloads, der er særligt følsomme over for ydeevne. Desuden kan du migrere din on-premises MySQL-, PostgreSQL-, MariaDB- og Apache Cassandra-dataejendom til Azure, samtidig med at du anvender avancerede garantier for sikkerhed, samme høje tilgængelighed for zone eller zoneredundant og garantier i serviceaftalen (SLA).

Pålidelighed

Azure-infrastrukturen består af geografiske områder, regioner og tilgængelighedszoner, som begrænser spændvidden for en fejl og dermed begrænser den potentielle effekt på kundeapplikationer og -data. Konstruktionen med Azure-tilgængelighedszoner blev udviklet for at levere en software- og netværksløsning til at beskytte mod datacenternedbrud og levere øget høj tilgængelighed (HA) til vores kunder. HA-arkitektur skaber en balance mellem høj robusthed, lav ventetid og omkostninger.

Vurder dine sikkerhedskrav, herunder behovet for at kryptere data, mens de er i brug. Med fortrolig Azure-databehandling kan du vælge mellem en bred vifte af hardware- og softwaremuligheder for at styrke sikkerheden i dine applikationer.

Du kan f.eks. bruge Azure VM'er®, der er baseret på Intel® Software Guard Extensions, til fortrolighed og tilpasning helt ned på applikationsniveau. Brug Azure-tjenester som f.eks. vores pålidelige startfunktion til at måle integriteten af den fortrolige VM. Tilføj Azure-attester, som er en samlet løsning, der verificerer virtuelle maskiners sikkerhedsforanstaltninger.

Sikkerhed

Som tidligere nævnt er sikkerhed altafgørende for de fleste applikationer og systemer – og endnu mere for forretningskritiske systemer, der ofte er kunderettede. Til cloud-tjenester som Azure og Microsoft 365 understøttes sikkerhed med Nul tillid-funktioner, der dækker hele platformen. Microsoft og deres partnere kan vurdere din Nul tillid-modenhed og overvåge, teste og forbedre din håndtering af sikkerhed og identitet, så du kan sikre, at sikkerhedspolitikker håndhæves i realtid.

Omkostningsoptimering og driftsmæssig fleksibilitet

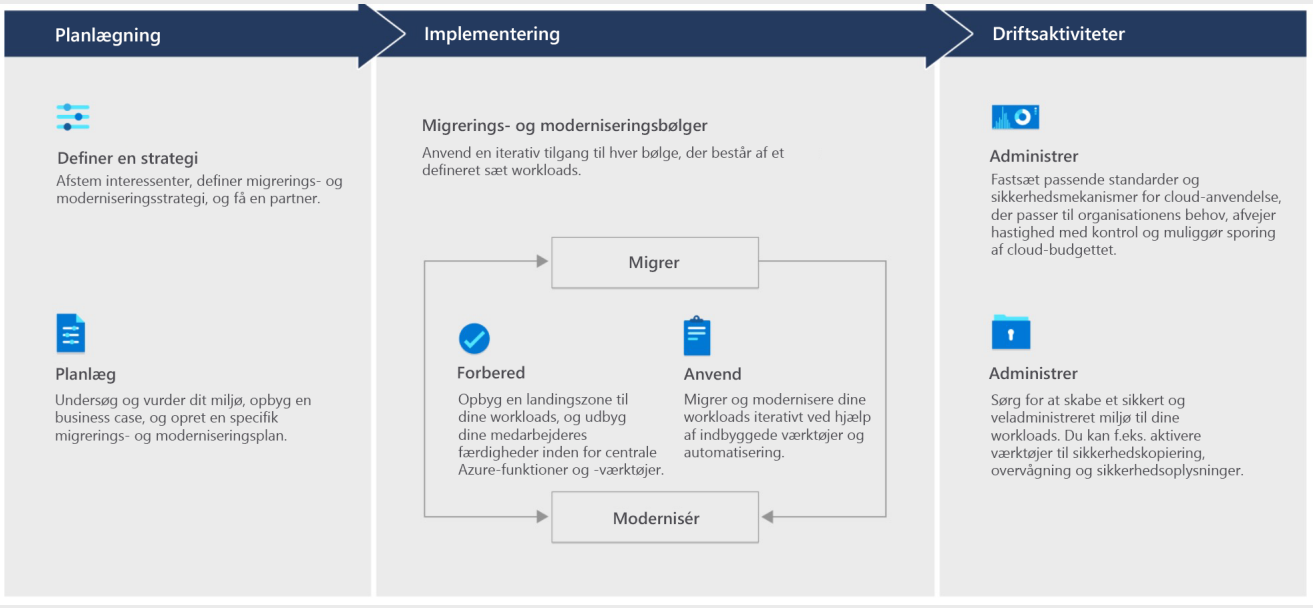
Din rejse mod en forretningskritisk cloud-løsning kræver muligvis, at du overvejer kompromiser. På den ene side ønsker du en robust og skalerbar løsning, der er meget sikker og overholder gældende krav til styring, risiko og overholdelse af regler og standarder. På den anden side skal du overholde organisationens retningslinjer for forretnings- og it-budgetter. Det er vigtigt at håndtere disse kompromiser inden for parametrene i din specifikke cloud-strategi. Ikke desto mindre kan flytning af din forretningskritiske infrastruktur til skyen øge den driftsmæssige fleksibilitet, især i et klima med forretningsmæssig usikkerhed eller ved pludselige udsving.

05

Overgang til skyen: Bedste praksis og mønstre

Planlægning, implementering og drift

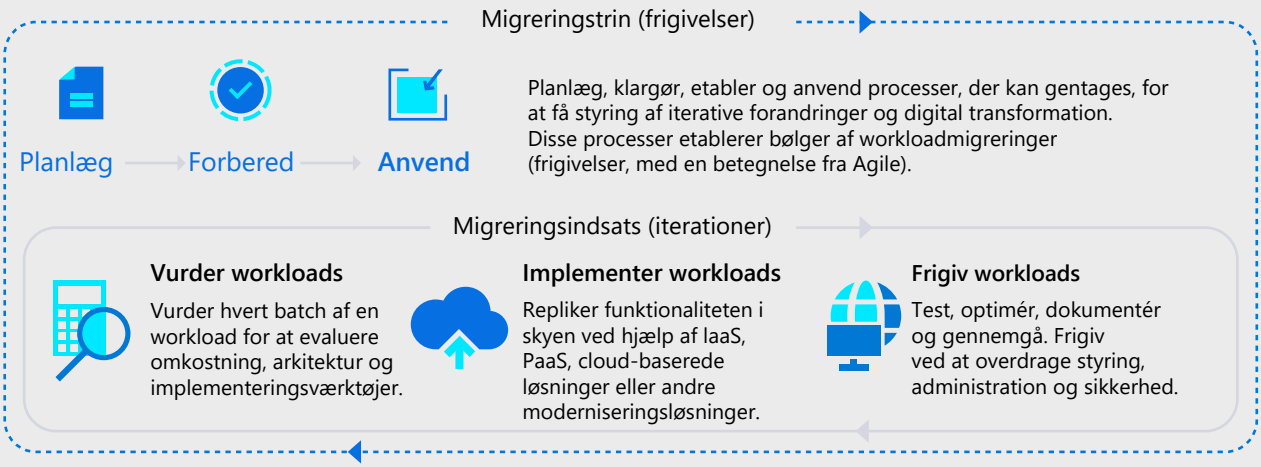
Cloud-migrering og modernisering er en løbende proces, der indebærer en betydelig forandringsproces i organisationen, og det gælder både mennesker, processer og teknologi. En samlet tilgang kan ikke kun hjælpe dig med at styre godt gennem rejsen, men også hjælpe med at sikre, at din organisation bliver opmærksom på de nye fordele – herunder effektivitet, smidighed og skalering – når dine workloads kører i skyen.



Figur 5. *Oversigt over Cloud Adoption Framework*

Overflytningen af forretningskritiske workloads til skyen kræver en systematisk proces og en fasebaseret tilgang. Brug tretrinsmetoden fra Cloud Adoption Framework-migreringsmetoden, som indeholder faserne Vurder, Implementer og Frigiv for migreringen af dine forretningskritiske workloads. Forstærk denne proces med tjeklister til forretningskritiske workloads.

Migrer



Figur 6. *Migreringsindsats: Vurder, Implementer og Frigiv*

Vurder workloads

Selvom du kan bruge Azure Migrate eller værktøjer fra uafhængig softwareleverandører (ISV) til at indsamle oplysninger om kildemiljøet, er det vigtigt at involvere applikationsarkitekterne, fageksperterne og eventuelt også applikationsleverandøren tidligt i migreringsprocessen.

Brug interviewprocessen, workshops eller whiteboarding-sessioner til at forstå applikationen arkitektur og kompleksitet, samt hvor forretningskritisk den er.

Implementer workloads

I denne fase af rejsen bruger du outputtet fra vurderingsfasen til at starte migreringen af miljøet. Denne vejledning hjælper med at identificere de relevante værktøjer til at nå til vejs ende på din rejse. Du vil udforske indbyggede værktøjer, tredjepartsværktøjer og projektledelsesværktøjer.

Tjekliste til vurdering af workloads

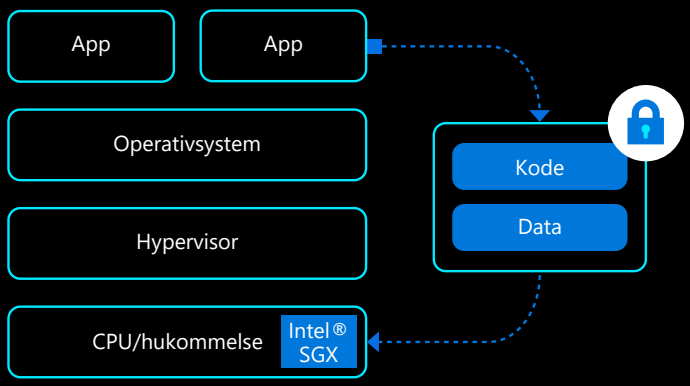
Planlægning

Når du har fuldført din vurdering, er det tid til at forberede dig til cloud-migreringen.

- ☐ Udarbejd målarkitekturen til hvert miljø. Udfør størrelsestilpasning for hvert miljø ved hjælp af Azure Migrate eller lignende værktøjer.
- ☐ Udarbejd omtrentlige omkostninger og ressourcer:
  - Bestem omkostningerne ved at køre workloads eller applikation på Azure-tjenester.
  - Identificer ressourcekrav (medarbejdere) til migreringen.
- ☐ Identificer tilgængelige nedetidsvinduer.
- ☐ Vælg de relevante Azure-abonnementer og -regioner til implementering af løsninger eller workloads.
- ☐ Vælg en strategi for cloud-implementering:
  - Identificer de systemkomponenter, der skal implementeres på Azure IaaS Virtual Machines.
  - Udpeg de systemkomponenter og grænseflader, der fortsat skal forblive on-premises.
  - Identificer de applikationskomponenter, der kan moderniseres og implementeres på Azure PaaS, f.eks. ved hjælp af Azure SQL Database, Azure App Service osv.
  - Afslut valg af databehandling, storage, netværk og database til understøttelse af dine forretningskritiske workloads.
- ☐ Fastlæg den relevante strategi for kryptering og foranstaltninger til styrkelse af sikkerheden. Desuden skal du oprette identitets- og sikkerhedskontroller.

Intel® Software Guard Extensions (Intel® SGX)-teknologi giver kunderne mulighed for at oprette enklaver, der beskytter data og holder data krypterede, mens CPU'en behandler dem. Operativsystemet (OS) og hypervisoren kan ikke få adgang til dataene. Datacenteradministratorer med fysisk adgang kan heller ikke få adgang til dataene.

Enklaver er sikrede dele af hardwarens processor og hukommelse. Du kan ikke se data eller kode inde i enklaven, selv med en debugger. Hvis kode, der ikke er tillid til, forsøger at ændre indhold i enklavehukommelsen, deaktiverer Intel® SGX miljøet og afviser handlingerne. Disse unikke funktioner hjælper dig med at beskytte dine hemmeligheder mod at være frit tilgængelige.



***Figur 7**. Oversigt over enklavestier*

Tænk på en enklave som en sikker bankboks. Du lægger krypteret kode og data ind i boksen. Udefra kan du ikke se noget. Du giver enklaven en nøgle til at dekryptere dataene. Enklaven behandler og krypterer dataene på ny, før de sendes ud igen.

Hver enklave har en krypteret sidecache (EPC) med en defineret størrelse. EPC'en afgør, hvor meget hukommelse en enklave kan rumme. VM'er i DCsv2-serien rummer op til 168 MiB. DCsv3/DCdsv3-seriens VM'er rummer op til 256 GB til mere hukommelseskrævende workloads.

- ☐ Analysér effekten af netværksventetid på applikationens ydeevne.
- ☐ Forstå kommunikationen med forskellige grænseflader og porte ved hjælp af værktøjer som Azure Migrate-afhængighedsanalyse, Service Map eller Cloudscape.
- ☐ Brug Service Map til at indsamle mængden af data og ventetid mellem forskellige grænseflader. Vurder effekten af ventetid, og identificer båndbreddebehovet.
- ☐ Udarbejd testplaner, hvis de ikke allerede findes.
- ☐ Identificer muligheder for at automatisere og standardisere implementeringsprocessen ved hjælp af værktøjer som Azure DevOps Pipelines, skabeloner til infrastruktur som kode (IaC), Jenkins, Ansible osv.
- ☐ Planlæg overvågning, programrettelser og opgraderinger samt backupløsninger.
- ☐ Udarbejd en strategi for høj tilgængelighed og disaster recovery.
- ☐ Planlæg teknisk uddannelse til support- og driftsteamet. Desuden skal du arrangere procestræning, hvis der sker ændringer i driftsprocesserne.
- ☐ Vær opmærksom på vigtige antimønstre:
    - Undgå at foretage funktionsforbedringer af applikationen under migreringsprocessen.
    - Undgå at foretage større ændringer af applikationens arkitektur under migreringsprocessen.

Implementering ved hjælp af infrastruktur som kode

Infrastruktur som kode er et sæt teknikker og praksisser, der hjælper it-fagfolk med at fjerne den byrde, der er forbundet med den daglige oprettelse og administration af modulær infrastruktur. Det giver it-fagfolk mulighed for at udarbejde og vedligeholde deres moderne servermiljø på en måde, der svarer til, hvordan softwareudviklere udarbejder og vedligeholder applikationskode.

- ☐ Implementer workloads i henhold til revideret og godkendt målarkitektur.
- ☐ Brug skabeloner til infrastruktur som kode og automatisering til at opbygge miljøet.
- ☐ Udfør eventuelle konfigurationer efter implementeringen.
- ☐ Udfør eventuelle foranstaltninger til styrkelse af sikkerheden efter migreringen.

Vigtig læring fra de seneste kundemigreringer

- Automatiser, automatiser, automatiser. Håndter alting som kode. Software, der ikke kan automatiseres, går i stykker.
- Bevar motivationen. Opbyg og implementer din infrastruktur, dine workloads og dine applikationer oftere.
- Alt, hvad der skal opbygges og implementeres, skal findes i kildekontrollen.
- Gør det til en vane at sætte ting i produktionen regelmæssigt.
- Undgå at gentage manuelle rettelser. Hver gang du har gjort noget for tredje gang, skal du automatisere det.
- Ingen test, som kan automatiseres, må forblive manuel. Dette omfatter enheds-, røg-, funktions- og end-to-end-test.
- Skab ensartethed i kommunikationen med regelmæssige scrum-opkald.
- Husk, at produktionsmiljøet skal kunne reproduceres efter behov, hvis det er nødvendigt.
- Fokusér på anvendelse og ændringsstyring for at håndtere kulturændringer i forbindelse med migrering af workloads til skyen.

Frigiv workloads

Denne fase giver også mulighed for at optimere dit miljø og udføre mulige transformationer af miljøet. Måske har du udført en migrering med "re-hosting", og nu, hvor dine tjenester kører på Azure, kan du se på løsningskonfigurationen eller de forbrugte tjenester igen med henblik på eventuelt at udføre "refactoring" for at modernisere og udvide funktionaliteten i din løsning.

Tjekliste til frigivelse af workloads

- ☐ Udnyt dine testplaner til at udføre ydeevnetest og dokumentere resultaterne. Sammenlign systemets ydeevne med en baseline for on-premises-ydeevne. Identificer eventuelle flaskehalse for ydeevnen, og foretag relevante ændringer, f.eks. ved at skalere Azure-ressourcer eller ved at tilføje cachelagring for at opnå hurtigere hentning af data.
- ☐ Udfør brugeraccepttest, og udfør test af høj tilgængelighed og disaster recovery.
- ☐ Brug passende fejlsporingssystemer som Azure DevOps eller Jira til at registrere, spore og løse eventuelle fejl. Dokumentér og løs eventuelle rapporterede problemer.
- ☐ Gennemgå workload-konfigurationer med henblik på dataoverholdelse og datasikkerhed.
- ☐ Føj potentielle forbedringer eller opdateringer til din DevOps-backlog.
- ☐ Udfør din eksekveringsplan:
  1. Udfør datasynkronisering og dataopdatering.
  2. Foretag det relevante skift til DNS.
  3. Omdiriger en del af brugertrafikken til ressourcer på Azure.
  4. Overvåg ydeevnematricerne.
  5. Gentag trin 3 og 4 for at omdirigere yderligere brugertrafik til Azure.
  6. Udfør den endelige eksekvering efter behov.
- ☐ Luk dine kildeservere ned.
- ☐ Optimer workloads over tid for at opnå yderligere driftsmæssig fleksibilitet:
  - Overvej at bruge cloudbaserede teknologier til overvågning og administration af dine applikationer.
  - Overvej at modernisere dine applikationskomponenter, så de kører på PaaS eller SaaS.
  - Brug betaling efter forbrug til de funktioner, hvor det er til din fordel. Nedskaler dit miljø efter behov.
  - Brug cloudbaserede værtøjer til omkostningsoptimering til at reducere omkostningerne ved at køre dine workloads.

Tjeklister til forretningskritiske workloads

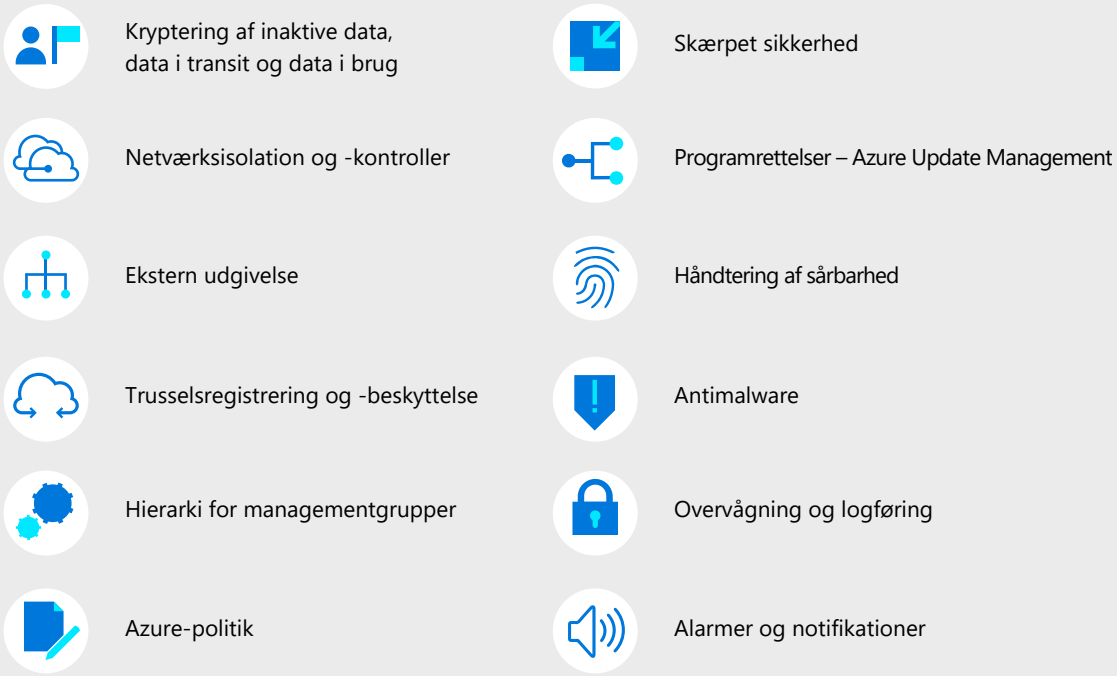
Følgende tjeklister indeholder bedste praksis for Azure-cloud-migrering, der gå ud over de grundlæggende cloudbaserede værktøjer. Disse tjeklister skitserer de fælles områder af kompleksitet, der ofte opstår i forretningskritiske workloads, og som kan kræve, at omfanget af migreringen udvides ud over Azure-migreringsvejledningen.

- ☐ VMware-migrering: Migrering af VMware-værter kan fremskynde den samlede migreringsproces. Hver migreret VMware-vært kan flytte flere workloads til skyen. Efter migreringen kan disse VM'er og workloads forblive i VMware eller migreres til moderne cloud-funktioner.
- ☐ SQL Server-migrering: Migrering af forekomster af SQL Server kan fremskynde den samlede migreringsproces. Hver migreret forekomst kan flytte flere databaser og tjenester og potentielt fremskynde flere workloads.
- ☐ Flere datacentre: Migrering af flere datacentre tilføjer betydelig kompleksitet. Under hver del af overflytningsprocessen (vurder, migrer, optimer og administrer) gennemgås andre overvejelser for at forberede sig på mere komplekse miljøer.
- ☐ Datakrav overskrider netværkskapaciteten: Virksomheder vælger ofte at migrere til skyen, fordi et eksisterende datacenters kapacitet, hastighed eller stabilitet ikke længere er tilfredsstillende. Men de samme begrænsninger gør migreringsprocessen mere kompleks, hvilket kræver yderligere planlægning under vurderings- og migreringsprocessen.
- ☐ Strategi for datastyring eller overholdelse: Når styring og overholdelse af regler og standarder er afgørende for en vellykket migrering, skal it-styringsteams og cloud-implementeringsteamet sikre yderligere tilpasning til hinanden.

Drift og sikkerhed

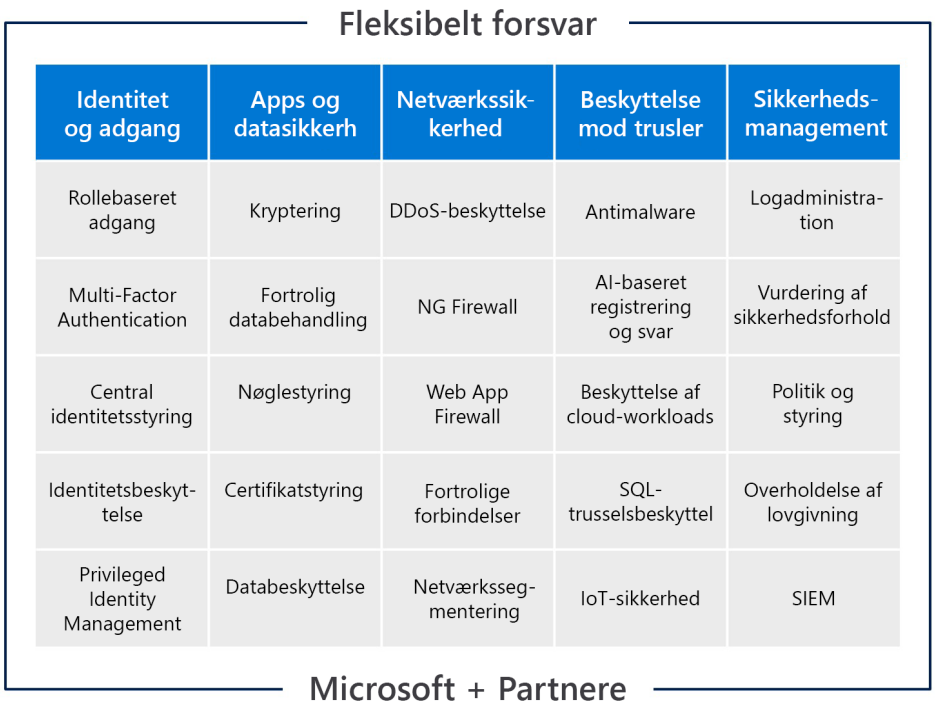
Driftssikkerhed dækker de driftsprocesser, der holder en applikation i gang i produktionen. Implementeringer skal være pålidelige og forudsigelige og automatiserede for at reducere risikoen for menneskelige fejl og samtidig sikre hurtige og rutinemæssige processer til at frigive nye funktioner og fejlrettelser. Muligheden for hurtigt at kunne rulle tilbage eller frem, hvis der er problemer med en opdatering, er lige så vigtig.

Følgende er de grundpiller, du skal overveje, før du påbegynder driftsrejsen:



Figur 8. *Tjekliste med de driftsmæssige grundpiller*

Med hensyn til sikkerhed skal du følge den dybdegående sikkerhedsløsning til at sikre alle dine workloads.



Figur 9. *Dybdegående sikkerhedsløsning*

Dybdegående indsigt til forretningskritiske workloads: Migrering af SAP til Azure IaaS

Lad os udforske forretningskritiske migreringspraksisser ved at dykke dybere ned i et eksempel på migrering af SAP til Azure. For mange virksomheder bruges SAP til at køre vigtige forretningsprocesser som f.eks. enterprise resource planning, customer relationship management og supply chain management. I nogle tilfælde er SAP-ejendommen stor og har komplekse indbyrdes afhængigheder. Derfor er det værd at undersøge som et forretningskritisk system, der kræver særlig opmærksomhed , når man migrerer til skyen. SAP er den perfekte kandidat til Azure Cloud Adoption Framework, da det ofte udgør en virksomheds "nerve- og kredsløbssystem".

Research

Sørg for, at du fuldt ud forstår designet og "størrelsen" af de nuværende on-premises SAP-systemer, så du kan tilpasse størrelsen og designet af destinationsmiljøet nøjagtigt.

Det er en almindelig udfordring at opdage små, men kritiske afhængige komponenter i gamle systemer, der går tabt i konfigurationsdatabaserne eller på grund af medarbejderudskiftning.

Brugerdefinerede systemer og apparater med "kildekode" kan også skabe udfordringer, da OEM-leverandøren muligvis ikke længere eksisterer, eller supporten droppes i forbindelse med en nyere pakke, hvilket kan kræve en større omlægning i forbindelse med migrering. Vær særligt opmærksom på ældre applikationer, der kører på ikke-x86/x64-platforme og løsninger med tilpasset kode.

Lær mere om SAP-workloads på Azure med tjeklisten til planlægning og implementering ›

Destinationsmiljø

Sørg for, at Azure-miljøet er blevet implementeret og grundigt testet, før du forpligter dig til at migrere og flytte SAP-systemer. Ved at følge den SAP-specifikke vejledning i Cloud Adoption Framework kan du få hjælp til din rejse mod skyen.

Lær mere om SAP på Azure på virksomhedsniveau ›

VM-størrelsestilpasning

Implementering af IaaS-VM'er skaber samme eller større ydeevne end on-premises, selvom SKU'er for den virtuelle maskine og disken kan skaleres op eller ned, i tilfælde af at kravene ændres.

- Brug SAP-værdierne, der leveres for at sikre, at VM-valget fungerer godt nok.
- Sørg for, at VM'en er certificeret af SAP (ikke alle VM'er er certificerede, men ikke-certificerede kan bruges i ikke-produktionsmiljøer).
- Sørg for at bruge SAP-certificerede OS-billeder.
- Design alle SAP-systemer med netværks- og storageventetid for øje.

For VM-hosting, HANA-databaser eller et tilsvarende in-memory-databaseprogram er det en generel regel at vælge en VM-størrelse, der understøtter en hukommelseskapacitet på mindst 1,2 x databasestørrelsen. Generelt kan du bruge vælgeren til den virtuelle maskine til at fremskynde processen til valg af VM og diskstorage.

Lær mere om størrelser på virtuelle maskiner på Azure ›

SAP på Azure-løsninger hjælper dig med at optimere din Enterprise Resource Planning (ERP) i skyen ved hjælp af sikkerhedsfunktionerne, pålideligheden og skalerbarheden i den SAP-certificerede infrastruktur i Azure.

Du kan vælge at implementere SAP-certificerede virtuelle maskiner on-demand til SAP NetWeaver-applikationer som SAP Business Suite og SAP HANA-baserede applikationer som SAP S/4HANA.

Du kan også vælge specialbygget SAP HANA-infrastruktur (SAP HANA Large Instances), som tilbyder højtydende databehandling, storage og netværk. HANA Large Instances drives af skalerbare Intel® Xeon® processorer og har fast Intel® Optane™ hukommelse (Intel® Optane™ PMem), som giver fordele som højere ydeevne og lavere TCO.

- SAP HANA-certificerede IaaS-forekomster med hukommelse fra 768 GB til 24 TB og fra 2 socket til 16 socket, der understøtter op til 896 vCPU'er.
- Certificering til SAP S/4HANA, SAP BW/4HANA, SAP BW på SAP HANA og Suite på SAP HANA.
- Brancheførende ydeevne med højtydende NFS-storage og -netværk.
- Høj tilgængelighed, disaster recovery, udskaleringskonfigurationer og indbygget understøttelse af backup.
- Snapshot-baserede backups af 24 TB database på få minutter.
- Kun public cloud, der tilbyder Intel® Optane™ PMem, som giver hurtigere indsigt, forenklet it-infrastruktur og lavere omkostninger.

Diske

Sørg for, at de diske, der er knyttet til VM'en, er funktionelle (IOPS, overførselshastighed osv.) til den specifikke applikation.

Lær mere om Azure Managed Disk-typer ›

Følgende tabel indeholder en sammenligning af de fire disktyper, som kan hjælpe dig med at beslutte, hvilken type du skal bruge.

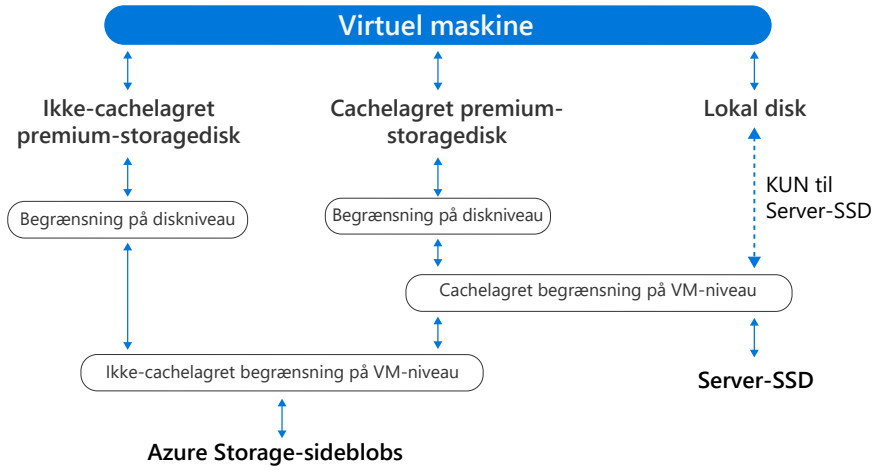
	Ultra-disk	Premium SSD	Standard SSD	Standard HDD
Disktype	SSD	SSD	SSD	HDD
Scenarie	IO-intensive workloads som SAP HANA, databaser på øverste niveau (f.eks. SQL, Oracle) og andre transaktionstunge workloads	Workloads, der er følsomme over for produktion og	Webservere, virksomhedsapplikationer med et lille forbrug samt udvikling/test	Sikkehedskopiering, ikke-kritisk, sjælden adgang
Maks. diskstørrelse	65.536 gibibyte (GiB)	32.767 GiB	32.767 GiB	32.767 GiB
Maks. gennemløb	2.000 MB/s	900 MB/s	750 MB/s	500 MB/s
Maks. IOPS	160.000	20.000	6.000	2.000

Figur 10. Sammenligning af disktyper for virtuelle maskiner

SAP-produktionssystemer bør følge retningslinjerne for anbefalet storagekonfiguration nedenfor, men den "omkostningsbevidste" indstilling kan bruges til ikke-produktionssystemer.

Sørg for, at den valgte kombination af VM og diskstorage er velegnet til at håndtere det gennemløb fra VM til diskstorage, som applikationen kræver. Dette er især vigtigt i scenarier med online-transaktion (OLTP).

Lære mere om storagekonfigurationer for SAP HANA Azure Virtual Machine ›



Figur 11. I/O-begrænsningskoncept

Lær mere om virtuelle maskiner og diskydeevne ›

Azure NetApp-filer (ANF)

Overvej at bruge ANF som supplement til Azure-diskmulighederne, hvor der kræves øget ydeevne og/eller meget lav RTO (Recovery Time Objective) eller RPO (Recovery Point Objective). ANF kan tilbyde ydeevne på op til 512 Mbps pr. 4 TB pulje på Ultra-niveau.

Lær mere om Azure NetApp Files ›

En vigtig fordel ved at bruge ANF er muligheden for straks at tage et øjebliksbillede af diskenheden uden at afbryde eksisterende diskhandlinger. Dette gør det meget hurtigt at udføre backup og gendannelse af meget store databaser. Azure tilbyder nu et værktøj til applikationskonsekvente øjebliksbilleder, der kan lette processen med backup, gendannelse og diskenhedskloning for øjebliksbilleder.

Lær mere om Azure Application Consistent Snapshot -værktøjet ›

Geninvester kapital fra reduceret TCO, der er opnået gennem forenklet it-infrastruktur og højere hukommelsestæthed.

Reducer drifts- og licensomkostningerne via nodekonsolidering med konfigurationer (Intel® Optane™ PMem).

Du kan køre SAP-installationer i ikke-forretningskritiske miljøer på samme hardware med separate storagetildelinger:

- Den bedst egnede løsning til dine behov og dit budget med den bredeste portefølje af certificerede SAP-muligheder
- Lavere TCO end ved en typisk on-premises-løsning – betal kun for det, du bruger
- Mere hukommelse til samme pris med en SAP HLI-opskaleringsløsning
- Fremragende ydeevne pr. krone, når du vælger Intel® teknologi til dine cloud-workloads

Se også: "Next Generation SAP HANA Large Instances with Intel® Optane™ drive lower TCO", april 2020. https://azure.microsoft.com/blog/next-generation-sap-hana-large-instances-with-intel-optane-drive-lower-tco/

Omkostninger

Når du har dimensioneret de påkrævede VM'er og tilknyttede ressourcer, er det vigtigt at beregne de samlede omkostninger for det, du planlægger at implementere, da det kan være mere end forventet. "Reserverede forekomster" og brugen af "omkostningsbevidste" muligheder kan hjælpe med at reducere det samlede månedlige forbrug.

Brug Prisberegneren i Azure til at bestemme priser korrekt for dine SAP-VM'er. OS-licensering er en væsentlig komponent i SAP-infrastrukturen. Brug betaling efter forbrug i stedet for BYOL (bring-your-own licensing) til Red Hat Enterprise Linux og SUSE Linux Enterprise.

Lær mere om omkostninger med Azure-prisberegneren ›

RTO/RPO

Forstå og dokumenter den krævede RTO og RPO til SAP-systemerne fuldt ud, og sørg for, at den løsning til backup, du planlægger at bruge, opfylder disse krav. Den indbyggede Azure-løsning til backup understøtter backup/gendannelse af SAP HANA-databaser.

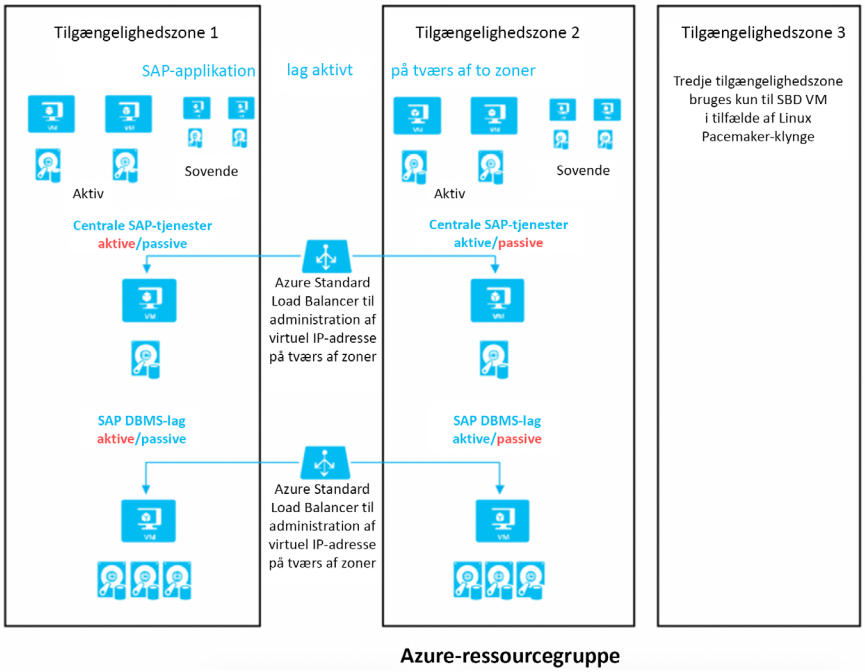
Hvis du vil have en meget lav RTO/RPO, kan du overveje at bruge Azure NetApp Files og funktionen til at tage øjebliksbilleder af diskenheder som understøttende diskenheder til dine workloads.

Lær mere om understøttelsesmatrixet til backup af SAP HANA-databaser på Azure VM'er ›

Lær mere om, hvordan Azure NetApp Files-øjebliksbilleder fungerer ›

Høj tilgængelighed

Overvej brug af flere serverforekomster og klynger for at give høj tilgængelighed sammen med tilgængelighedszoner, der kan hjælpe med at yde beskyttelse mod tab af datacentre i en bestemt region. Dette er især vigtigt for HANA-databaseforekomster.



Figur 12. *SAP-konfiguration, der bruger Azure-tilgængelighedszoner*

Lær mere om konfiguration af SAP-workloads med Azure-tilgængelighedszoner ›

Disaster recovery

Det er vigtigt at planlægge, designe og gennemteste disaster recovery, før du migrerer nogen SAP-produktionssystemer. Dette er med til at sikre, at de centrale systemer bliver ved med at køre, og at de hurtigt kan bringes online igen i en anden region. Disaster recovery-websteder skal testes regelmæssigt med test-failover-aktivitet for at sikre DR-tilstanden.

Når du bruger ANF, kan SnapMirror-diskenheden bruges til at replikere dine diskenheder til en anden NetApp-diskenhed i en parret region. Replikeringen kan konfigureres på helt ned til 10 minutter med en RPO på 20 minutter for landskaber, hvor et SAP HANA-systemreplikeringswebsted har en overkommelig pris.

Lær mere om replikering af Azure NetApp File-diskenheder på tværs af regioner ›

Test

Når de nye SAP-systemer er blevet implementeret og konfigureret, er det afgørende at udføre så mange tests som muligt, før du migrerer. Dette skal omfatte funktionstest samt ydeevnetest og kræver input fra SAP Basis-teamet og produktejere/interessenter.

Sikkerhed

Infrastruktursikkerhed bør medtages som en del af designet/implementeringen af landingszonen. Den bruger en kombination af rollebaseret adgangskontrol (RBAC) og politikker til at håndhæve de krævede retningslinjer og adgangen. SAP-sikkerhedslaget kan derefter tilføjes eller migreres over dette som en del af migreringsprocessen.

Lær mere om sikkerhed i Microsoft Cloud Adoption Framework til Azure ›

Forretningstilpasning

Risikoindsigt

Integrer sikkerhedsindsigt i risikostyringsprocessen og digitale initiativer.

Sikkerhedsintegration

Integrer sikkerhedsindsigt og -praksisser i forretnings- og it-processer. Integrer sikkerhedsdiscipliner sammen.

Robusthed i virksomheder

Sørg for, at organisationen kan fungere under angreb og hurtigt genvinde fuld driftsstatus.

Sikkerhedsdiscipliner

Adgangsstyring

Opret adgangsmodel med Nul tillid til moderne og ældre aktiver ved hjælp af identitets- og netværkskontroller.

Sikkerhedsdrift

Registrer, reager på og genopret efter angreb. Søg efter skjulte trusler. Del trusselsefterretninger bredt.

Beskyttelse af aktiver

Beskyt følsomme data og systemer. Opdag, klassificer og beskyt aktiver løbende.

Sikkerhedsstyring

Identificer, mål og administrer sikkerhedsstillinger løbende for at reducere risici og opretholde overholdelse af standarder.

Innovationssikkerhed

Integrer sikkerhed i DevSecOps-processer. Afstem praksis for sikkerhed, udvikling og drift.

Figur 13. *Sikkerhedsmetode til SAP og Cloud Adoption Framework*

Styring

På samme måde som sikkerhed bør styring inkluderes som en del af infrastrukturens design/implementering ved hjælp af managementgrupper, politik og RBAC.

Lær mere om styring i Microsoft Cloud Adoption Framework til Azure ›

Administrer

Definer virksomhedspolitik

Forretningsrisici

Dokumentér lurende forretningsmæssige risici og organisationens tolerance over for risici baseret på dataklassificering og applikationsvigtighed.

Politik og overholdelse af regler og standarder

Konverter risikobeslutninger til politikerklæringer for at fastlægge grænser for anvendelse af cloud-løsninger.

Behandle

Etabler processer til at overvåge overtrædelser og overholdelse af virksomhedspolitikker.

Fem discipliner inden for styring af cloud-løsninger

Omkostningsstyring

Evaluer og overvåg omkostninger, begræns it-forbruget, skalér for at imødekomme behov, skab ansvarlighed i forhold til omkostninger.

Sikkerhedsbaseline

Sørg for overholdelse af kravene til it-sikkerhed ved at anvende en grundlæggende sikkerhedsbaseline på alt anvendelsesarbejde.

Ensartede ressourcer

Sørg for konsekvens i forhold til konfigurationen af ressourcer. Håndhæv praksis for onboarding, genoprettelse og synlighed.

Identitetsbaseline

Sørg for, at baseline for identitet og adgang håndhæves ved konsekvent at anvende rolledefinitioner og tildelinger.

Implementeringsacceleration

Fremskynd implementering ved hjælp af centralisering, ensartethed og standardisering på tværs af installationsskabeloner.

Figur 14. *Cloud Adoption Framework-styringsmodel*

Implementering

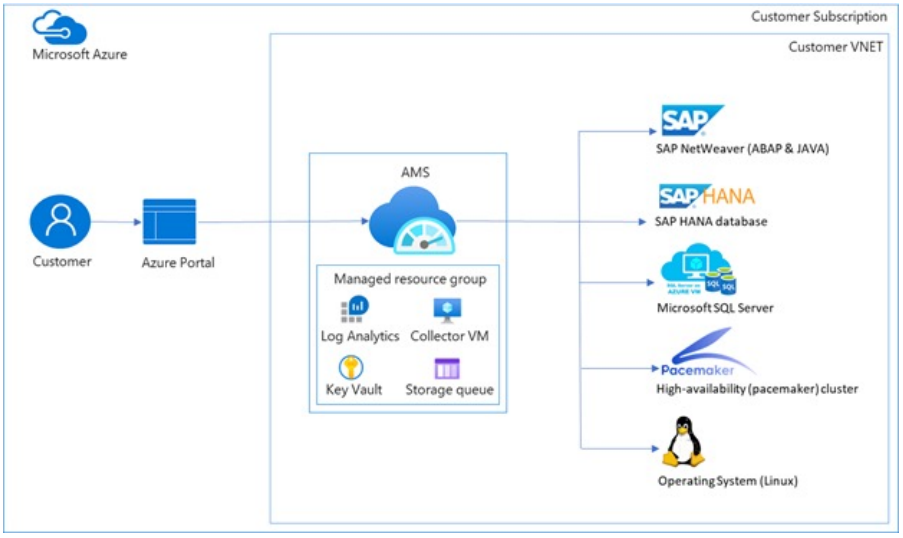
Undgå manuel implementering, når det er muligt. Udnyt SAP HANA-implementeringsværktøjerne til at automatisere implementeringen af din SAP-infrastruktur, og udnyt de inkluderede Ansible-drejebøger til at implementere SAP Basis Foundation. Kombiner disse med Azure Cloud Adoption Framework Terraform-værktøjer til at automatisere og lette implementeringen af de mest komplekse miljøer.

Hvis du vil forenkle produktionen til ikke-produktionsrelaterede opdateringsaktiviteter, skal du tilskynde til anvendelse af DevOps og en teknisk tilgang til webstedets pålidelighed. Opbyg pipelines i Azure DevOps for at automatisere regelmæssigt forekommende opgaver, som f.eks. ikke-produktionsrelateret implementering og opbygning af tests.

Overvågning

Overvej at bruge den SAP-specifikke overvågningsløsning (i øjeblikket i prøveversion) til at overvåge de forskellige logfiler og målinger fra den nye infrastruktur. Sørg for, at de virtuelle maskiner og de tilknyttede ressourcer er konfigureret til at sende alle oplysninger til et Log Analytics-arbejdsområde.

Få mere at vis om overvågning af SAP på Azure ›



Figur 15. *Azure Monitor til SAP-løsninger*

06

Forretningskritisk partnerøkosystem

Mange organisationer, som vi samarbejder med, er ivrige efter at realisere utallige fordele for deres egne forretningskritiske applikationer, men først skal de besvare spørgsmål om deres rejse mod cloud-løsningen, herunder:

- **Er de kerneapplikationer, jeg bruger on-premises, certificerede og understøttede på Azure?**
- **Når jeg flytter til Azure, kan jeg så bevare det samme niveau af applikationstilpasning, som jeg har opbygget i årenes løb on-premises?**
- **Vil mine brugere opleve nogen effekt på ydeevnen af mine applikationer?**

I bund og grund ønsker du at sikre, at du fortsat kan udnytte det strategiske samarbejde, du har opbygget med dine partnere og ISV'er, når du skifter dine centrale forretningsprocesser til skyen. Du ønsker at fortsætte med at bruge de samme applikationer, som du har brugt mange år på at tilpasse og optimere on-premises.

Microsoft forstår, at kørsel af dine forretninger på Azure dækker over mere end de tjenester og funktioner, som enhver platform kan levere. Du har brug for et omfattende økosystem. Azure har altid været partnerorienteret, og vi styrker fortsat vores samarbejde med et stort antal ISV'er og teknologipartnere, så du kan køre de applikationer, der er afgørende for din virksomheds drift på Azure.

Vi samarbejder med mange partnere om at udarbejde effektive migreringsstrategier, -planer og -tjenester til meget komplekse og forretningskritiske workloads. Vores in-house-teams kan understøtte alle faser af din forretningskritiske migreringsrejse. Vi udvider de mange måder, hvorpå vi yderligere kan levere værdi til din organisation.

Selvom vi samarbejder med ISV'er og globale og regionale systemintegratorer, arbejder vi også mere specifikt med værktøjsleverandører for at understøtte automatiseret registrering, workload-analyse og meget mere. Da Azure understøtter mange open source-systemer, kan vi udnytte partnerskaber, der specialiserer sig i disse typer løsninger.

Læs vores blogindlæg, der giver en dybdegående oversigt over vores forretningskritiske partnerskaber ›

07

De næste trin

Vi håber, at du med denne e-bog føler dig bedre forberedt på at modernisere dine forretningskritiske systemer og applikationer med en cloud-løsning. Vi har identificeret forretningskritiske apps og systemer og forklaret risiciene og fordelene ved at flytte dem til skyen på baggrund af foreslåede migrerings- og moderniseringsmetoder. Se de næste trin nedenfor og ressourcerne i tillægget for at lære, hvordan Microsoft kan hjælpe med din cloud-transformationsrejse.

Overvejer du migrering af dine forretningskritiske workloads?

Kontakt en Microsoft-partner for at få mere at vide om Azure-cloud-tjenester og -programmer, der kan hjælpe med at understøtte din cloud-transformationsrejse. Læs, hvordan et partnerskab med Microsoft kan hjælpe dig med at udvikle en sikker og pålidelig migreringsstrategi for dine forretningskritiske workloads.

Kom i gang med Cloud Adoption Framework til Azure ›

Er du i gang med undersøgelser til din første migrering af forretningskritiske workloads?

Hvis du udforsker migrering af forretningskritiske workloads til Azure, kan en Microsoft-partner hjælpe dig med at planlægge og oprette en Azure-landingszone i virksomhedsskala til at afprøve dine indledende forretningskritiske workloads. Du kan også fortsætte med at opbygge kvalifikationer inden for Azure-udvikling og -drift ved at lære om Azure-cloud-tjenester og -programmer, som kan understøtte en pålidelig og sikker cloud-transformationsrejse.

Lær mere om Azure Migration & Modernization Program ›

Er du klar til at flytte forretningskritiske workloads til Azure?

Hvis du er klar til at starte migreringen af forretningskritiske workloads i stor skala, kan du planlægge en Envisioning-workshop om cloud-transformation med en Microsoft-partner i dag. Vi kan hjælpe med at opbygge og udføre en køreplan for dit migreringsengagement og yde support til din cloud-transformationsrejse.

Kom i gang med Azure-cloud-transformation ›
(kun på engelsk)

08

Tillæg: Ressourcer

Disse ressourcer giver vores kunder de nødvendige værktøjer og oplysninger til effektivt at administrere og migrere deres workloads til Azure.

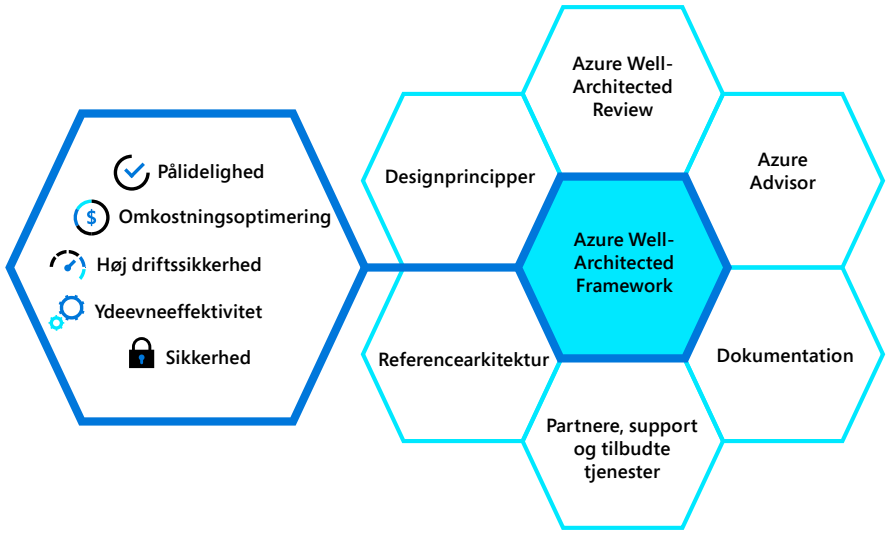
Well-Architected Framework

Azure Well-Architected Framework (WAF) er et sæt grundprincipper, der kan bruges til at forbedre kvaliteten af workloads. Strukturen består af grundpiller for arkitektonisk kvalitet: omkostningsoptimering, driftseffektivitet, ydeevneeffektivitet, pålidelighed og sikkerhed. Indarbejdelse af disse grundpiller hjælper med at producere stabile og effektive cloud-arkitekturer i høj kvalitet.

WAF-grundpille	Beskrivelse
Omkostningsoptimering	Administration af omkostninger for at maksimere den leverede værdi.
Høj driftssikkerhed	Driftsprocesser, der holder et system kørende i produktion.
Ydeevneeffektivitet	Et systems evne til at tilpasse sig ændringer i belastningen.
Pålidelighed	Et systems evne til at genoprette efter fejl og fortsætte med at fungere.
Sikkerhed	Beskyttelse af applikationer og data mod trusler.

Figure 16. *Grundpillerne i Well-Architected Framework*

Lær mere om Microsoft Azure Well-Architected Framework ›



Figur 17. *Azure Well-Architected Framework*

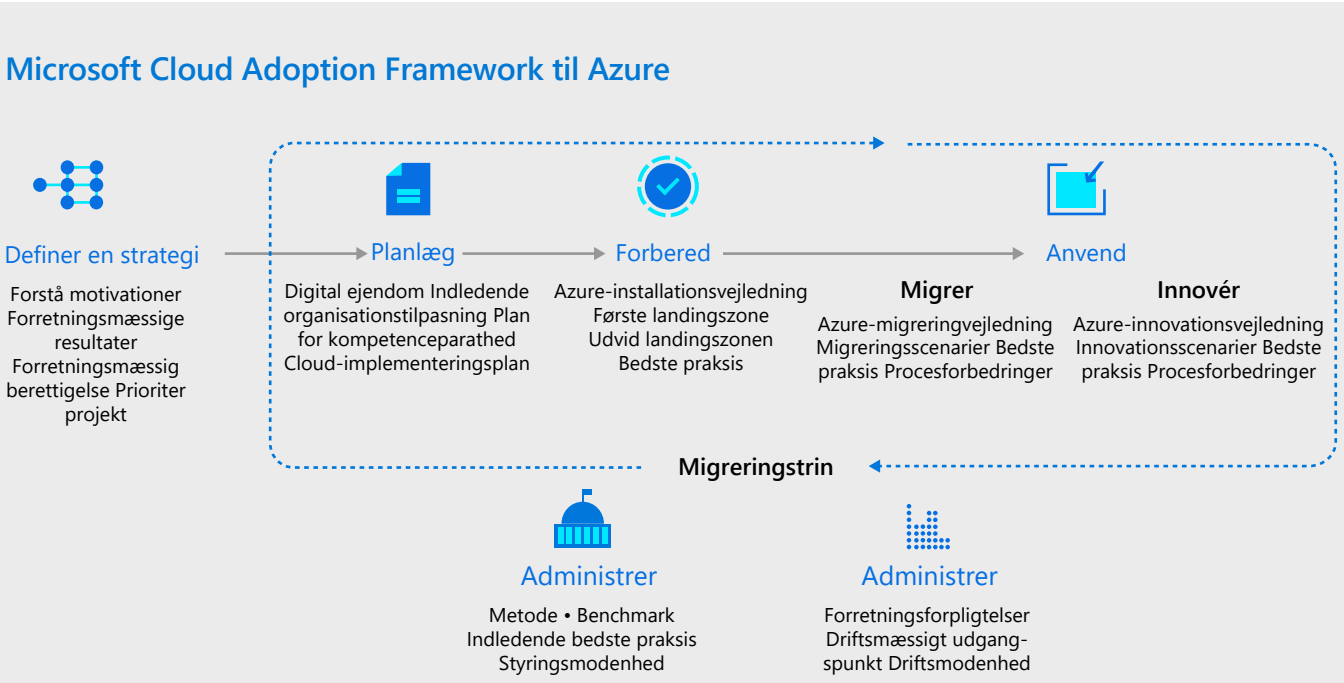
Cloud Adoption Framework

Cloud Adoption Framework til Azure er en samling af dokumentation, tekniske vejledninger, bedste praksis og værktøjer, der hjælper med at koordinere strategier for forretningen, organisatorisk parathed og teknologi. Denne koordinering understøtter en klar og handlingsrettet rejse mod skyen, der hurtigt leverer de ønskede forretningsresultater.

Cloud Adoption Framework hjælper kunderne med at foretage en forenklet cloud-rejse i fire hovedtrin:

1. Definer en strategi
2. Planlæg
3. Klargør
4. Implementer

Lær mere om Cloud Adoption Framework ›

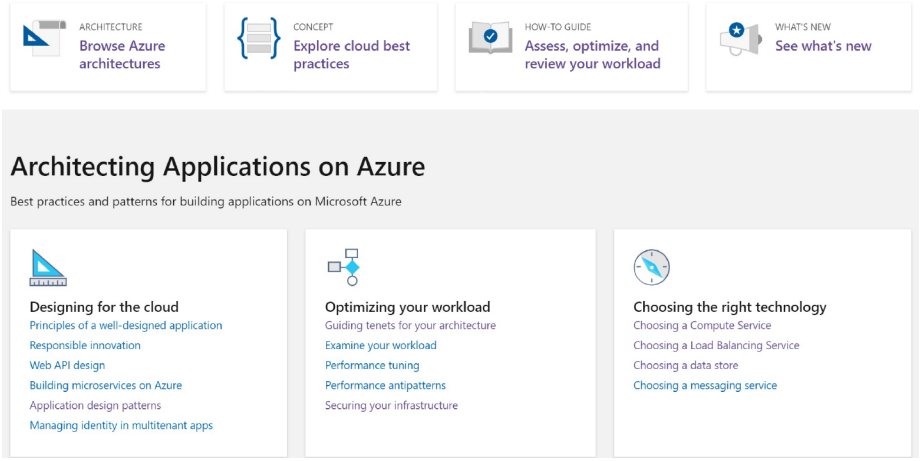


Figur 18. *Oversigt over Cloud Adoption Framework*

Arkitekturcenter for Azure

Arkitekturcenter for Azure er en nyttig ressource til at gennemse alle arkitekturmønstre og finde de bedste fremgangsmåder til at bygge applikationer på Microsoft Azure.

Læs mere om de teknologiske områder i Arkitekturcenter for Azure ›



Figur 19. *Arkitekturcenter for Azure*

Vejledning om arkitektur for SAP på Azure

Vejledning om arkitektur for SAP på Azure beskriver et sæt grundprincipper, der bruges til at sikre kvaliteten af SAP-workloads, der kører på Azure. Denne vejledning er baseret på Microsoft Azure Well-Architected Framework, men anbefalingerne er specifikke for implementeringer af SAP-løsninger. Et solidt arkitekturfundament starter med de fem grundpiller for kvalitet: omkostninger, DevOps, robusthed, skalerbarhed og sikkerhed.

- Oversigt
- SAP HANA på Azure (Large Instances)
- SAP HANA-opskalering på Linux
- SAP NetWeaver i Windows på Azure
- SAP S/4HANA i Linux på Azure
- SAP BW/4HANA med Linux-VM'er på Azure
- SAP NetWeaver på SQL Server
- SAP-implementering på Azure ved hjælp af en Oracle DB
- Udvikling/test af SAP-workloads på Azure

Cloud-vurdering og risikovurdering

Kunderne kan evaluere deres forretningsstrategier og modtage skræddersyet vejledning fra Microsoft Assessments.

- Azure Well-Architected Review
- Cloud Journey Tracker
- Developer Velocity
- Governance Benchmark
- Strategic Migration Assessment and Readiness Tool

Læs om de tilgængelige vurderinger ›

Lær mere om risikovurdering med vejledningen til overholdelse af regler og standarder i Microsoft-cloud-løsningen ›

Offentlige case studies

- USA | Albertsons | Detailhandel | Microsoft Customer Story—Albertsons and Microsoft partner on cloud adoption to enable digital transformation
- Storbritannien | Bristol City Council | Offentlig sektor | Microsoft Customer Story—Bristol City Council unlocks its ability to innovate and sets the stage for true digital transformation
- Mexico | SAE | Microsoft Customer Story—SAE Digital Transformation Initiative
- Storbritannien | Benenden School | K–12 | Microsoft Customer Story—Benenden School adopts hyperconverged infrastructure and remote learning with Azure Stack HCI and Intel
- USA | MobileCoin | Banker og kapitalmarkeder | Microsoft Customer Story—MobileCoin creates fast, trusted cryptocurrency transfers with Azure confidential computing
- Storbritannien | Buro Happold | Professionelle tjenester | Microsoft Customer Story—Buro Happold creates sustainable, striking environments with Azure high-performance computing fueled by Intel
- Canada | Royal Bank of Canada | Banker og kapitalmarkeder | Microsoft Customer Story—RBC creates relevant personalized offers while protecting data privacy with Azure confidential computing
- Kundehistorier om SAP på Azure-løsninger
- Kundehistorier om forretningskritiske applikationer på Azure

Programmer og tilbud

- AMMP: Azure Migration and Modernization Program
- Cloud Transition Services: Accelerating modernization and enabling innovation on the Microsoft cloud (English only)

Microsoft