PEDAGOGISK RAMMEVERK FOR CLOUD COMPUTING

Første del

A-CCT

Delfinansiert av
Den europeiske union

acctproject.eu

Maja Pucelj, Annmarie Gorenc Zoran, Nadia Molek, Ali Gökdemir, Ioan Ganea, Christina Irene Karvouna, Petter Grøttheim, Leo Mršić, Maja Brkljačić, Monika Rohlik Tunjić, Alojz Hudobivnik

PEDAGOGISK RAMMEVERK FOR CLOUD COMPUTING

FØRSTE DEL

Novo mesto, 2023

Delfinansiert av
Den europeiske union

DOI: 10.37886/a-cct-no

PEDAGOGISK RAMMEVERK FOR CLOUD COMPUTING - FØRSTE DEL

Maja Pucelj, Annmarie Gorenc Zoran, Nadia Molek, Ali Gökdemir, Ioan Ganea, Christina Irene Karvouna, Petter Grøttheim, Leo Mršić, Maja Brkljačić, Monika Rohlik Tunjić, Alojz Hudobivnik

Fagfellevurderere: Faculty of Organisation Studies in Novo mesto

Tilgjengelig kl: https://www.fos-unm.si/si/dejavnosti/zaloznistvo/

Kataložni zapis o publikaciji (CIP) pripravili v Narodni in univerzitetni knjižnici v Ljubljani
COBISS.SI-ID 178826243
ISBN 978-961-6974-88-2 (PDF)

Delfinansiert av
Den europeiske union

2021-1-SI01-KA220-VET-000034641

Innhold

INNHOLDET I TABELLENE

INNHOLD I FIGURENE

ORDLISTE

Uttrykk	Engelsk uttrykk	Betydning
Agility	*Agility*	Agility, eller smidighet, i sammenheng med cloud computing refererer til den raske og effektive kapasiteten til skyressurser og -tjenester for å tilpasse seg utviklende forretningsmessige og teknologiske krav.
Backend	*Backend*	Komponentene på serversiden i et skybasert program. Den omfatter mange funksjoner som datahåndtering, implementering av forretningslogikk, applikasjonsvert og databehandling. Disse backend-komponentene fungerer sammen med den brukervendte frontend, noe som letter driften og funksjonaliteten.
Backhaul	*Backhaul*	Nettverksryggraden fungerer som en kanal for overføring av data til den sentrale kjernen i nettverket.
Sikkerhetskopier data	*Back-up data*	Dataduplisering er prosessen med å opprette en ekstra kopi av data som allerede er lagret på et annet sted, med det formål å redusere risikoen for tap av data.
Blockchain	*Blockchain*	En distribuert hovedbok som registrerer alle transaksjoner som skjer i et nettverk.
Blowfish	*Blowfish*	Et symmetrisk nøkkelblokkchiffer brukes for å sikre sikker overføring av data.
Bucket	*Bucket*	En logisk enhet for lagring av data i objektlagringsystemer, for eksempel AWS S3.
Cloud computing	*Cloud computing*	Utnytte beregningsressurser, for eksempel servere, lagring og databaser, via internettbasert infrastruktur ofte referert til som "skyen".
Cloud computing teknologier	*Cloud computing technologies*	Teknologiene som letter utnyttelsen av databehandlingstjenester via internett.
Klynge	*Cluster*	Et nettverk av sammenkoblede datamaskiner som samarbeider tett for å utføre aktiviteter.
Holdbarhet	*Durability*	Dataholdbarhet refererer til kapasiteten til et system for å forhindre tap av data innen en spesifisert tidsramme.
Elastisitet	*Elasticity*	Kapasiteten til dynamisk å tildele databehandlingsressurser basert på den rådende arbeidsbelastningen.

Brannmur	*Firewall*	En nettverkssikkerhetsenhet som utfører funksjonene til å overvåke og filtrere både innkommende og utgående nettverkstrafikk.
Fleksibilitet	*Flexibility*	Kapasiteten til effektivt og fleksibelt å tilpasse seg endringer og svingninger i arbeidsmengden.
Frontend	*Frontend*	Komponentene knyttet til brukergrensesnittet og brukeropplevelsen innenfor et gitt system.
Flux	*Flux*	Flux er den nye generasjonen av skalerbar desentralisert skyinfrastruktur.
Topptekster	*Headers*	Innledningen, som vanligvis brukes til å inkludere rutingsinformasjon, er et ekstra sett med data som ligger i begynnelsen av en datapakke.
Helse	*Health*	Den nåværende tilstanden eller funksjonelle tilstanden til et system eller en prosess.
Helsekontroller	*Health checks*	Implementering av overvåkingssystemer er avgjørende for å sikre at tjenestene opererer på sitt høyeste effektivitetsnivå.
Helsesonde	*Health probe*	En testforespørsel utføres for å verifisere responsen og den generelle helsen til en tjeneste.
Hub	*Hub*	Et mye brukt grensesnitt for å etablere tilkobling mellom enheter i et nettverk.
Industriell revolusjon	*Industrial revolution*	Den nevnte tiden betegner en betydelig fase av industriell utvikling, kanskje med henvisning til konseptet Industri 4.0 innenfor et moderne informasjonsteknologisk rammeverk. Dette paradigmet omfatter integrering av internett av ting og cloud computing.
IT-teknologi	*IT technology*	Utnyttelse av datasystemer og telekommunikasjonsteknologi med det formål å lagre, hente, overføre og manipulere data.
Latency	*Latency*	Tidsforsinkelsen som oppleves i et system.
Lytter	*Listener*	Et nettverksovervåkingssystem eller en protokoll som aktivt oppdager og svarer på nettverkstilkoblinger og forespørsler.
Lokalt datanettverk	*Local computer network*	Et lokalnett (LAN) refererer til et nettverk som omfatter et begrenset geografisk område, for eksempel en bolig, arbeidsplass eller utdanningsinstitusjon.
Stormaskin	*Main frame computer*	Et databehandlingssystem med høy ytelse som brukes til utførelse av beregningsintensive oppgaver i stor skala.
Kartlegging	*Mapping*	Prosessen med å etablere et forhold mellom elementer som tilhører ett sett og elementer som tilhører et annet sett.

Patch	*Patch*	En programvareoppdatering som er ment å rette opp eller forbedre funksjonaliteten.
Proxy	*Proxy*	En mellomliggende server som fungerer som en mellommann mellom sluttbrukerklienter og destinasjonene de får tilgang til for surfeformål.
Push-kode	*Push code*	Handlingen med å overføre kode til et lager eller miljø med det formål å gjennomføre endringer.
Ruting	*Routing*	Prosessen med å fastslå ruten for datapakker å krysse i et nettverk.
Skalerbarhet	*Scalability*	Et systems evne til å utvide og tilstrekkelig håndtere et økt etterspørselsnivå.
Skaleringssett for virtuelle maskiner	*Virtual machine scale sets*	Azure-databehandlingsressursen det refereres til, er en plattform som gjør det mulig for brukere å distribuere og overvåke en samling virtuelle maskiner som ikke kan skilles.
Virtuelle maskiner	*Virtual machines*	En datasystemsimulering er en programvarebasert representasjon som replikerer egenskapene til en fysisk datamaskin.

1 INTRODUKSJON

I år 2021 mottok prosjektpartnere fra Slovenia, Kroatia, Nederland, Norge, Romania og Tyrkia det europeiske Erasmus+prosjektet med tittelen: "Digital innholdsutvikling for integrering av skyteknologier i formell og fjernfaglig utdanning". Et av resultatene av prosjektet er også kursinnhold om skyteknologier, støttet av eksempelapplikasjoner, utarbeidet som en veiledning for lærere i formell og fjernfaglig utdanning. Nedenfor finner lærerne en første del av de nevnte retningslinjene.

I dette dokumentet vil lærerne finne en rekke verdiforslag som prosjektpartnerne har identifisert som de mest hensiktsmessige for å begynne å lære elevene om skytjenester. Fokuset har vært på konvergens av bransjer i dag, slik at lærerne vil finne en kombinasjon av beste praksis fra ulike bransjer for å gi elevene skreddersydde løsninger med maksimal effektivitet for elevene. Temaene i innholdet i skyundervisningsmaterialet er som følger: 1. Introduksjon til Cloud Computing og typer Cloud Computing, 2. Priser vs markedssammenligning mellom AWS, Azure og GCP, 3. Distribuere servere og belastningsbalansere på alle databehandlingsplattformer, 4.Lagringstjenester på AWS, Azure og GCP, 5.Sikkerhetstjenester - Identitets- og tilgangsadministrasjon, 6.Typer nettverkstjenester og innstilling av dem, 7.Databasetjenester på AWS, Azure og GCP, 8.Domeneoppsett og 9.Overvåkings- og varslingstjeneste.

Nedenfor kan læreren også finne 61 praktiske eksempler på applikasjoner, egnet for å lære VET-studenter om skyteknologi. I vedlegg 1 kan en lærer finne enda et detaljert eksempel på applikasjoner, og i vedlegg 2 kan en lærer finne kodebiter for noen av applikasjonene nedenfor, som lærere kan bruke som maler som gjør det lettere for dem å forklare elevene hvordan de skriver inn gjentatte kodemønstre.

2 OPPLÆRINGSMATERIELL FOR DATABEHANDLING I SKYEN

2.1 Introduksjon til cloud computing teknologier og typer cloud computing

Vanskelighetsgrad: Lett
Fullføringsperiode: timer
Mål:
Etter å ha lest materialet, vil leseren forstå begrepet cloud computing som det oppfattes i IT-teknologi og de viktigste tjenestene den inkluderer. Du vil også kjenne til de viktigste fordelene og ulempene ved cloud computing-teknologier.

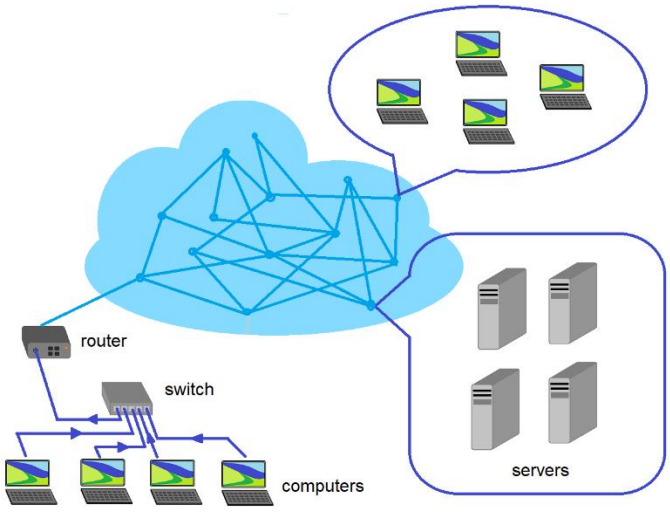
Prestasjoner
Etter å ha fullført denne søknaden, vil du kunne:

- kjenne til historien til begrepet cloud computing,
- forstå betydningen av begrepet cloud computing,
- kjenn tjenestene som tilbys av skyteknologier,
- kjenne til fordeler og ulemper ved cloud computing-teknologier.

Fra og med den første industrielle revolusjonen utviklet det menneskelige samfunn som helhet seg og vitenskapelig fremgang fortsatte. Menneskeheten har gått gjennom tre industrielle revolusjoner, hver med sine egne egenskaper. Begynnelsen av det tredje millenniet er preget av fremveksten av den fjerde industrielle revolusjonen karakterisert av storskala bruk av industriroboter, kunstig intelligens og cloud computing-teknologier.

Alle disse tingene bringer dype forandringer i folks aktivitet og liv. Hvis begrepene roboter og kunstig intelligens er noe antydende og ikke gir mye tvetydighet, synes begrepet cloud computing å være mer sjargong enn et teknisk begrep. Og likevel har dette begrepet en viktig teknisk betydning for IT-bransjen.

Begrepet sky er faktisk en metafor for begrepet Internett. Videre er ikonet relatert til Internett representasjonen av en sky, og det betyr alt som finnes i Internett-teknologi usett av brukeren. Med andre ord ønsker ikonet å uttrykke det faktum at alt som tilhører Internett er skjult i en tåke for Internett-brukeren.



Figur 2.1. Tankevekkende bilde av begrepet cloud computing

Cloud computing-teknologier skaper en spesiell innvirkning på økonomiske aktiviteter over hele verden. Selv om den umiddelbare betydningen av dette begrepet vil være datalagringstjenesten på en server hos et selskap som har teknisk evne til å lagre data trygt, er hele begrepet cloud computing bredere. Den har sin opprinnelse i øyeblikket da datasystemer dukket opp.

Således, ifølge flertallet av forskere og forskere, ville begrepet cloud computing ha blitt oppgitt i en veldig enkel form i 1955 da en datavitenskapsmann kom opp med ideen om at visse dataressurser skulle deles mellom ulike brukere gjennom utleie fordi IT-teknologier på den tiden hadde ublu kostnader og mange brukere ikke hadde råd til å kjøpe dem. Denne ideen tilhører forskeren John McCarthy og regnes som begynnelsen på begrepet cloud computing.

Fjorten år senere utviklet en annen forsker J.C.R. Licklider det lokale datanettverket i institusjonen der han jobbet, som nå regnes som forfedre til Internett. Formålet med Lickiders nettverk var å legge til rette for utveksling av IT-ressurser (programvare og data) mellom forskere fra den respektive institusjonen. McArthys konsept med å leie IT- og nettverksressurser realisert av J.C. R. Licklider for utveksling av IT-ressurser førte til utviklingen av det vi i dag kaller Internett. Opprinnelig ble dette kalt Ethernet.

I 1972 skapte IBM den første stormaskinen VM/370 eller Virtual Machine Facility/370. Enhver forsker eller forsker kunne få tilgang til dataene som er lagret på dette systemet ved hjelp av et Hercules-emuleringsprogram. Hvis frem til 80-tallet i forrige århundre datateknologi var tilgjengelig bare for forskere, forskere eller store selskaper, men i perioden 1980-1989 oppstod hjemmedatamaskiner og teknologiene som ble brukt til å skape kommunikasjonsnettverk mellom datamaskiner ble forbedret. Kommunikasjonsnettverket ble kalt Ethernet og var standardisert. Noen selskaper som Ms_Dos og Novel har gitt et viktig bidrag til forbedring av kommunikasjonsnettverk mellom datamaskiner. IT-ressursene var vert på servere som kunne nås fra hvor som helst og av alle som hadde et datasystem koblet til datanettverket.

Internett vokste eksponentielt mellom årene 1990-1998. I 1996 introduserte en gruppe forskere fra Compaq Computer-selskapet begrepet cloud computing for første gang. Lanseringen av SalesForce.com-applikasjonen i 1999 gjorde det mulig å selge informasjon til samarbeidende selskaper eller lagre den via en nettportal. Dette var begynnelsen på en periode der andre selskaper begynte å tilby de samme tjenestene og bidro til forbedring av Internett. Utseendet på markedet for dataprodukter av Web Services som tilbys av Amazon var et viktig øyeblikk. Denne tjenesten tilbød datalagring, tilgang til programmer og virtualisering.

Mellom 2006 og 2012 konsoliderte Google-selskapet sin tilstedeværelse på Internett-tjenestemarkedet ved å lansere Google Apps. I 2011 annonserte Apple-selskapet lanseringen av sin egen datalagringsløsning på servere som er tilgjengelige via Internett under navnet Apple iCloud. Et år senere ble Google Drive-applikasjonen lansert av Google-selskapet, som forente alle fasilitetene som tilbys under en enkelt tjeneste.

Mellom 2012-2017 ble skytjenester utvidet, og på grunn av utseendet på mobile enheter med høy ytelse ble skytjenester tilgang til flere og flere brukere, noe som stimulerte IT-selskaper til å forbedre tjenestene som tilbys. Forskningen innen IT har ført til økningen av det tekniske nivået på nettverkene for dataoverføring, og dermed har hastigheten på Internett også økt.

I dag brukes begrepet sky mer og mer uten å vite sin sanne betydning i IT. Den enkleste definisjonen av begrepet cloud computing er å ha enkel tilgang til IT-ressurser (programmer og data) eller til andre tjenester som ikke er installert på din egen datamaskin. For hjemmeforbrukeren kan skytjenester bety tilgang til elektroniske posttjenester, lagring av data i Google Disk eller bruk av spesialiserte tjenester for overføring av store filer som ikke kan sendes via e-post (f.eks. Det kan også bety tilgang til filmer, musikk eller spill via Internett.

Fra synspunktet til noen små og mellomstore bedrifter kan cloud computing-tjenester defineres ved sikker lagring av programvare og egne data på steder utenfor selskapet som lett kan nås fra hvor som helst og av alle som er autorisert av selskapets ledelse. Dette gir betydelige økonomiske fordeler for selskapet fordi det ikke er nødvendig for det å kjøpe eget utstyr for datalagring eller programvare, og det er heller ikke nødvendig for tilstedeværelse av spesialister for å administrere spesifikke IT-aktiviteter.

For å fjerne tvetydigheter i definisjonen av begrepet cloud computing, definerte US National Institute of Standards and Technology (NIST) cloud computing-tjenester i 2011 som følger:
"Cloud computing er en modell for å muliggjøre allestedsnærværende, praktisk, on-demand nettverkstilgang til en delt pool av konfigurerbare databehandlingsressurser (f.eks. Nettverk, servere, lagring, applikasjoner og tjenester). Den kan raskt klargjøres og utgis med minimal ledelsesinnsats eller samhandling mellom tjenesteleverandører".

NIST spesifiserte også fem viktige egenskaper som cloud computing må ha:

- selvbetjening på forespørsel;
- bred nettverkstilgang;
- ressurs pooling;
- rask elastisitet eller ekspansjon;
- Målt tjeneste.

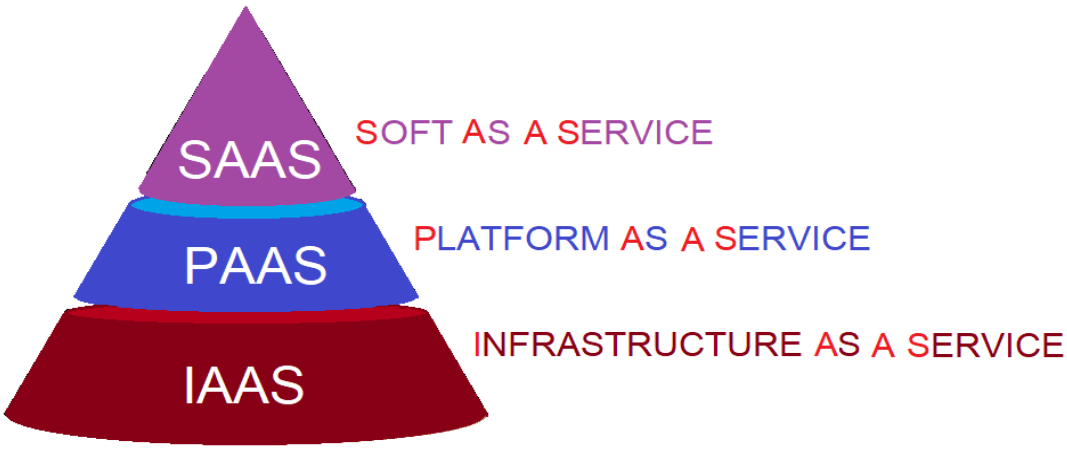
Cloud computing-tjenester kan leveres av et selskap som arbeider i IT-feltet eller kan nås av et selskap med en annen IT-profil, av enkeltpersoner eller av lokalsamfunn.
Derfor definerte NIST fire typer cloud computing:

- offentlig;
- privat;
- fellesskap;
- hybrid,

Hver av de fire typene skydatabehandling som er spesifisert ovenfor, kan tilby følgende grunnleggende tjenester:

- programvare, (Software as a Service) – (SaaS);
- plattform (Platform as a Service) – (PaaS);
- Infrastruktur (Infrastructure as a Service) – (IaaS);

Innenfor en cloud computing-tjeneste som tilbyr alle de tre grunnleggende tjenestene som er oppført ovenfor, er de strukturert som vist på bildet nedenfor (se figur 2.2 nedenfor):



Figur 2.2. Hierarkiet på de tre grunnleggende nivåene i skydatabehandlingstjenester

I tillegg til de tre tjenestene som er vist så langt, tilbyr IT-selskaper også andre tjenester som har følgende navn og akronymer:

- Gaming as a Service (GaaS).
- Communications as a Service (CaaS).
- Database as a Service (DBaaS).
- Desktop as a Service (DaaS).
- Hardware as a Service (HaaS).
- Identity as a Service (IDaaS).
- Storage as a Service (STaaS).

I det følgende vil vi forklare definisjonen av hver tjeneste:

- Software As A Service (SAAS) består av å tilby tjenester som: Gmail, Youtube eller andre lignende tjenester til brukeren. Ved å bruke disse tjenestene betales noen ganger en tilgangsavgift eller de er gratis.
- Platform As A Service (PAAS) tilbyr programvareutviklere en plattform for å skrive koder for forskjellige applikasjoner og teste dem på den plattformen.

- Infrastructure As A Service (IAAS) er en tjeneste som består i å fremleie servere og nettverk til et selskap som igjen kan tilby dem som tjenester til andre brukere.
- Gaming As A Service (GAAS) er en tjeneste levert av enkelte selskaper der brukere kan få tilgang til programvare som tilbyr morsomme spill i det virtuelle miljøet. Denne programvaren kan kjøres på datamaskiner eller mobile enheter.
- Communications as a Service (CAAS) er meldingstjenester, videokonferanser for samfunn hvis medlemmer ikke er på samme sted eller ekstern kommunikasjon via tale eller tekst. Denne kategorien inkluderer applikasjoner som de som tilbys av Skype, Facebook eller Twitter.
- Database as a Service (DBAAS) betyr levering av databasetjenester som involverer lagring av data som tilhører selskaper, lokalsamfunn eller enkeltpersoner på serverne til IT-selskaper som spesialiserer seg på denne forbindelse. Disse dataene kan enkelt og trygt nås av dataeieren. Dataeieren betaler en leieavgift for denne tjenesten. Tjenesten er lønnsom fordi opprettelse og styring av en spesialisert database for et bestemt felt krever en spesiell økonomisk innsats for mange selskaper.
- Desktop As A Service (DAAS) er en tjeneste der en bestemt person kan bruke datamaskinen sin ved å få tilgang til den fra en annen enhet når han er på et annet sted. Prosessen kalles virtualisering og gir tilgang til en datamaskin under Windows, Mac eller Linux operativsystemer gjennom skyteknologi, ved hjelp av ikoner, snarveier, etc. på datamaskinen du har fått tilgang til.
- Hardware As A Service (HAAS) gjør det mulig for et selskap å leie maskinvare fra en leverandør. Alle maskinvareelementer: datamaskiner, skrivere, mobiltelefoner, nettbrett, etc. er eiendommen til leverandøren i løpet av den tiden de brukes av selskapet som leide dem. Denne tjenesten anses å være en del av skyteknologi, selv om den virker forskjellig fra andre teknologispesifikke tjenester.
- Identity As A Service (IDAAS) sikrer sikker tilgang til IT-ressurser gjennom programvare som identifiserer fingeravtrykks- eller irisdeteksjon av personen som ønsker tilgang til dataene. I tillegg til disse elementene som brukes til gjenkjenning, kan det være andre prosedyrer for å verifisere identiteten til personen som ber om tilgang til de lagrede dataene.
- Storage As A Service (STAAS), Google Drive og Dropbox er to eksempler på denne typen tjenester. I prinsippet tillater denne tjenesten lagring av data som tilhører ansatte i et selskap eller enkeltpersoner. Disse dataene kan nås når som helst av eieren, noe som garanterer datasikkerhet.

Som det er nevnt ovenfor, anses begrepet sky som en metafor for Internett. Over tid, i tillegg til kommunikasjonstjenestene mellom datamaskiner kjent som Internett, (som krevde eksistensen av et nettverk og spesialisert programvare), opprettet selskaper flere fasiliteter som senere ble tjenester. Begrepet sky kan referere til de lokale internettnettverkene til noen selskaper som tilbyr IT-tjenester i et geografisk område eller til hele internettnettverket spredt over hele kloden. Som et resultat kan vi snakke om en lokal sky og en generell sky. På verdensmarkedet er det fire gigantiske selskaper som tilbyr cloud computing-tjenester. Disse er: Microsoft med Microsoft OneDrive-tjenesten, Amazon som tilbyr Cloud Services-tjenesten, Apple tilbyr

iCloud-tjenesten og Google som tilbyr Gmail, Drive, etc. Tjenester. I tillegg til disse kommer Dropbox Cloud-tjenestene.

En IT-bedrift kan velge å lage sitt eget lokale skysystem som de kan leie ut til sluttbrukere som kan være enkeltpersoner, lokalsamfunn eller bedrifter med en annen aktivitetsprofil enn IT.

Et cloud computing-system består av:

- Det lokale Internett-nettverket til én eller flere brukere. Alle datamaskiner, skrivere og andre maskinvarekomponenter til en bruker er koblet til én eller flere lokale brytere.
- Ruteren er enheten som brukerens switch er koblet til internettjenesten til en Internett-leverandør (Internet Service Provider).
- En portal eller et nettsted sikrer tilkoblingen til selskapets skytjeneste som har sine egne lokale servere og servere. I selskapets skyservere kan data lagres, eller programvare kan kjøres. Kommunikasjon mellom selskapets servere og brukeren skjer gjennom en frontend-portal. Alle selskapets skyservere er sammenkoblet og danner en klynge. Serverklynger kan være plassert hvor som helst i verden og kan være plassert på forskjellige steder i store avstander fra hverandre.

Selskapet som eier serverklyngene sørger for sikker brukertilgang, vedlikeholder databasen og oppdaterer programmene som tilbys klientene. En enklere definisjon av en skytjeneste er et datasenter der hundrevis av servere er sammenkoblet som gir muligheten til å lagre og kjøre programvare som selskaper eller enkeltpersoner har gratis eller betalt tilgang til. I tillegg til muligheten for å lagre data eller kjøre applikasjonsprogramvare, kan skytjenester også tilby noen av tjenestene som er oppført ovenfor.

Figur 2.3. Aspekter i et datasenter som tilbyr cloud computing-tjenester

Bruken av cloud computing-tjenester som tilbys av et IT-selskap har følgende fordeler:

- **Enkel tilgang fra hvor som helst i verden**. Dataene som er lagret på serveren, kan nås fra hvor som helst i verden av personen som eier dataene. Betingelsen er at personen har tilgang til Internett og har en enhet som de kan få tilgang til Internett gjennom.
- **Redusere selskapets kostnader** fordi selskapet ikke trenger å investere i kjøp av maskinvareutstyr og ansette IT-spesialister for å lage programvare og administrere databaser. Mange ganger er kostnaden ved investeringen i maskinvare- og programvareutstyr større enn fordelene med å ha servere lokalt.
- **Fleksibilitet -** karakteriserer det faktum at funksjonene i programvaren eller brukergrensesnittene enkelt kan endres i henhold til kundens ønsker. Dette kan føre til forbedrede forretningsresultater.
- **Permanent oppdatering av IT-teknologi.** IT-teknologiene knyttet til databasene, men også til programvaren som brukes til overføring av databasene, er i kontinuerlig utvikling. Leverandører av skydatabehandlingstjenester anskaffer ny teknologi for å holde tritt med den tekniske utviklingen. Dermed kan brukeren av skytjenester dra nytte av de siste nyhetene innen disse teknologiene.
- **Beskyttelse av data ved** naturkatastrofer som rammer eierselskapet. Data og programvare som brukes av et selskap, eller et fellesskap kan gå tapt hvis en brann eller en naturkatastrofe påvirker selskapet som eier dataene hvis de er lagret på servere eller andre lokale enheter. Siden selskapets data er lagret på servere som ligger i avstand fra eierselskapet, er dataene trygge.
- **Samarbeid mellom ansatte i et selskap eller flere selskaper** gjennom tilgang til programmer eller data. Ansatte i et selskap som samarbeider om et prosjekt, kan enkelt få tilgang til de samme dataene som er lagret på serveren mye lettere.
- **Datasikkerhet**. Tilgang til data eller programmer som er lagret på serverne til et IT-selskap, er sikret og basert på tilgangspassord. Hvis dataene som er lagret på serveren, ble holdt på et lokalt lagringssystem, CD-ROM, pinne eller til og med i en bærbar datamaskin, fører tap eller tyveri til uopprettelig tap av data. Selskapet som tilbyr skytjenestene tar også strenge tiltak for å stoppe tilgangen til uautoriserte personer til de lagrede dataene.

Selv om cloud computing-tjenester har fordeler som anbefaler at de brukes i stor skala, har disse tjenestene også noen ulemper. Disse ulempene er:

- Oppdatering av programvaren som styrer driften av serverne kan føre til tap av lagrede data. Et eksempel er en hendelse fra 2011 da Amazon-selskapet mistet kundenes data.
- Mangelen på tilkobling til Internett er en stor ulempe, for den personen som er på et sted der han ikke har tilgang til Internett, kan han ikke bruke dataene fra serveren.
- Når det gjelder noen selskaper som tilbyr skytjenester, kan utgiftene øke og tvinge selskapet til å suspendere tjenestene som tilbys til klienter.
- Manglende evne til å få tilgang til et selskaps server selv om Internett-tilkoblingen er mulig. Det skjedde tidligere, selv hos kjente selskaper der meldingen HTTP Error 503ș Serveren er utilgjengelig dukket opp. Heldigvis skjer dette sjelden.

- Myndighetenes tilgang til person- eller bedriftsdata. Regjeringer kan tvinge cloud computing-selskaper til å gi dem tilgang til data lagret på serverne sine for å få konfidensiell informasjon om borgere eller selskaper som har data lagret på disse serverne. For å opprettholde hemmeligholdelsen av de lagrede dataene, har noen selskaper flyttet serverne sine til andre staters territorier og kommer dermed ut av jurisdiksjonen til staten som ber om tilgang til dataene som er lagret på serverne deres.
- Servere kan angripes av hackere. I dette tilfellet er datasikkerheten i fare. Det har vært situasjoner der kjente personer klaget over at deres personlige data lagret på serverne til skyselskaper ble stjålet.
- Til tross for alle ulempene som er nevnt ovenfor, blir cloud computing-tjenester i økende grad brukt over hele verden, og mange selskaper i IT-feltet investerer for å øke kvaliteten på cloud computing-tjenester.

2.2 Priser vs. markedssammenligning mellom AWS, Azure og GCP

Vanskelighetsgrad: Lett
Ferdigstillelsesperiode: 45 minutter per enhet, 4 enheter i modulen

Mål:

Cloud computing er et av de hotteste trendordene i IT-bransjen akkurat nå, da skyleverandører tilbyr fordelene med enkelt oppsett, høy skalerbarhet og overkommelig pris overalt.
Følgende enheter i denne modulen vil gjøre deg kjent med de beste skyleverandørene som er tilgjengelige på markedet i dag. Amazon Web Services (AWS), Google (GCP) og Microsoft (Azure) er de mest kjente offentlige skyleverandørene og har milliarder av dollar i markedsandel i cloud computing.
Når vi går gjennom enhetene, vil vi gå fra en generell oversikt over disse 3 leverandørene til en fokusert analyse av hva de tilbyr for prisen. Det er en kjennsgjerning at banebrytende skyløsninger kommer med en pris, som ikke er annerledes for disse tre store leverandørene - AWS, Azure og Google - da vi vil analysere hvordan prisene varierer i henhold til deres planer, tjenestevalg, funksjoner, rabattalternativer, ressursbruk og mer.

Prestasjoner

Etter å ha fullført denne modulen vil du kunne:

- Forstå etterspørselen etter cloud computing-plattformer,
- gjenkjenne deres innflytelse i bedriftsledelsessektoren, blant andre,
- gjenkjenne noen av likhetene og forskjellene mellom skyplattformene fra et teknisk perspektiv,
- Lær om markedstilstedeværelsen til de 3 plattformene, sammenlignet med hverandre,
- Lær hvordan prisalternativer etableres og hvordan de er relatert til markedets etterspørsel etter 2019.

2.2.1 Hva tilbyr Cloud Computing?

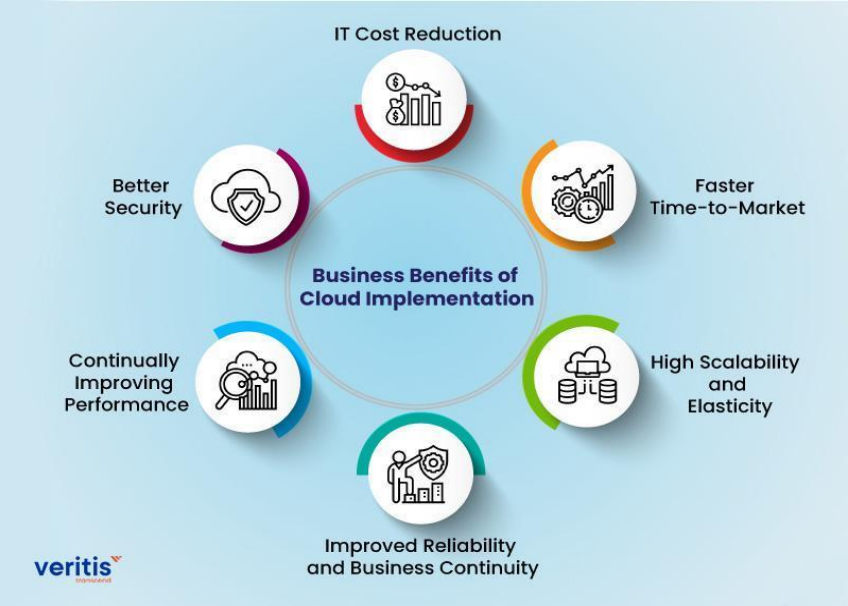
Hvorfor vil du henvende deg til en skyplattform for dine behov? Denne enheten ser på hva cloud computing gir for noen som deg selv, håper å administrere en bedrift, eller leter etter noen form for IT-assistanse.

La oss snakke om det grunnleggende.
Disse plattformene er like i viktige faktorer for hvorfor de dominerer markedet, men hver av de tilbyr forskjellige ressurser når det gjelder databehandling, nettverk og lagringsalternativer.
Det er klart at når du leter etter den beste cloud computing-plattformen for virksomheten din, er det viktig å holde oversikt over dine mål, forventet vekst og budsjett.

Hva tilbyr cloud computing?
La oss se på noen av hovedgrunnene til at skydatabehandling er bra for det du trenger når du hjelper deg med å administrere en bedrift:

- Reduserte IT-kostnader: Med skyimplementeringer trenger du bare å betale for databehandlingskapasitet i henhold til forretningsbehovene dine, noe som reduserer de løpende kostnadene ved innkjøp, distribusjon, vedlikehold og administrasjon av lokal infrastruktur.
- Raskere tid til markedet: Skyen aktiveres på få minutter. Ingen ventetid på å komme i gang.
- Høy skalerbarhet og fleksibilitet: Skyimplementeringer kan automatisk skalere arbeidsbelastninger som svar på endrede markedskrav.
- Forbedring av virksomhetens pålitelighet: Implementering av sikkerhetskopiering av data og nødgjenoppretting i skyen er vanligvis mye enklere, billigere og mindre forstyrrende enn lokalt som er risikabelt og tidkrevende.
- Kontinuerlige ytelsesforbedringer: Fordi det er i sanntid, oppdateres skyinfrastrukturen regelmessig med den nyeste og kraftigste maskinvaren for databehandling, lagring og nettverk.
- Sørg for sikkerhetstiltak: Oppfyll enkelt grunnleggende krav til sikkerhet og samsvar med det mest fleksible og sikre skymiljøet som er tilgjengelig i dag.

Dette bildet nedenfor viser hvordan bruk av skyen reduserer kostnadene for IT generelt i å administrere en bedrift, og hvorfor det er så attraktivt for brukerne:



Figur 2.4. Forretningsfordeler med skyimplementering

Her er noen grunnleggende definisjoner av de tre leverandørene:

Hva er AWS Cloud Platform?
AWS, eller Amazon Web Services, er en skytjenesteplattform fra Amazon som tilbyr databehandling, lagring, levering og andre tjenester til brukere. Til sammen kan alle disse SaaS- (Software-as-a-Service), Infrastructure-as-a-Service (IaaS) og Platform-as-a-Service (PaaS)-tilbudene effektivt brukes av deg, da de tilbyr følgende funksjoner:

- 18,000+ tjenester,
- datautregning,
- oppbevaringsløsninger,
- integrering av skyapper,
- analyse og maskinlæring,
- produktivitetsverktøy,
- utvikler- og administrasjonsverktøy.

Amazon Web Services er den mest populære lagringstjenesten for objektarkiver, noe som er en hovedårsak til at den dominerer det nåværende skymarkedet. Den består av verktøy for IoT, sikkerhet, database, administrasjon, analyse, bedriftsapplikasjoner og mer.

Fra Amazon kommer tre separate nivåer av utviklerstøtte, forretningsstøtte og bedriftsstøtte, og tilbyr en kombinasjon av verktøy, skyteknologi og eksperter.

Mange av AWS styrker er knyttet til posisjonen som en ledende leverandør av moderne skytjenester og det store omfanget av den globale virksomheten. Til sammen drev disse faktorene AWS sin vekst og gjorde det mulig for selskapet å tilby en stor liste over non-stop-tjenester til bedrifter over hele verden.

Her er noen av styrkene til AWS:

- Støtter alle større operativsystemer, inkludert macOS (i motsetning til andre leverandører)
- Tilbyr et bredt spekter av tjenester
- Fortsatt vekst i tjenestetilbudet
- Sofistikert og lett tilgjengelig
- Kan håndtere et stort antall sluttbrukere og ressurser
- Veldig lett å få tilgang til og starte.

Her er noen av ulempene:

- En relativt høy kostnad
- Tilleggskostnader for viktige tjenester
- Tilleggskostnad for teknisk kundestøtte
- Bratt læringskurve etter å ha engasjert plattformen.

Microsoft Azure

Siden det også er en integrert plattform på skyen som tilbyr lagring, de samme databasemulighetene og databehandling som Amazon gjør, har den også forskjellige skytyper som imøtekommer spesifikke krav. Det er et av de beste alternativene i skyen for selskaper som trenger mye datalagringsplass, med alternativer som Data Lake Storage og Queue Storage. Masselagring er ideell for bedrifter med en stor mengde ustrukturert data, mens fillagring er ideell for bedrifter med spesifikke fillagringskrav. Azure tar basen fra gjeldende Microsoft Office Suite-programvare, et annet forretningsverktøy for å tilby følgende funksjoner, i et konfigurert format-

- En utviklingsplattform i skyen
- Blockchain-teknologi
- Prediktiv programvare
- Verktøy for IoT-integrasjon.

En viktig funksjon i Azure, akkurat som Amazon, er den lagdelte tilnærmingen til støttetjenester, som inkluderer en utviklerplan som tilbyr ubegrenset støtte i arbeidstiden, og standardplanen, som også inkluderer ubegrenset tilgang. For mer strukturert støtte for bedrifter er den profesjonelle planen for skyen det beste alternativet.

Brukere liker de spesielle funksjonene i Azure på grunn av:

- Utbredt tilgjengelighet

- Kuponger for servicekontrakter for brukere av Microsoft-databehandling i skyen
- Intuitiv konfigurasjon med Microsoft-familien av programvare
- Innebygde apper som støtter flere språk (inkludert Java, Python, .NET og PHP).

Noen av problemene som kan oppstå inkluderer:

- Mangelfull datahåndtering
- Rapporter om problemer med kjernenettverket
- Noen mennesker tror det er vanskeligere å mestre enn andre plattformer
- Designet kan virke mindre profesjonelt enn på andre plattformer
- Rapporterte problemer med teknisk støtte.

Google Cloud Platform (GCP)

På grunn av sin endeløse IT-ekspertise og interne forskning har Google vist seg å være en markedskonkurrent. Den har mange vertsbaserte tjenester som plattform som en tjeneste (PaaS) og infrastruktur som en tjeneste (IaaS) for databehandling, lagring og applikasjonsutvikling.

Google ble først offentliggjort i 2004, men det har først nylig begynt å utgjøre en alvorlig trussel mot både AWS og Azure.

GCP tar raskt igjen konkurrentene takket være Googles omfattende globale tilstedeværelse og tilsynelatende ubegrensede kapasitet til innovasjon.

For øyeblikket tilbyr den tjenester som:

- Administrere produktivitet i bedrifter og andre områder
- Lagring av data
- Studio for utvikling av skyapplikasjoner
- Motorer for AI og maskinlæring, for eksempel skytale-API, visuelt API og andre
- Forretningsanalyse og andre tilleggskomponenter.

I motsetning til de to andre tjenestene er Googles lagringsalternativer ganske enkle, med skylagring og vedvarende disklagring som avrunder listen. I tillegg til sin egen interne overføringstjeneste, gir Google også brukere tilgang til et økende antall online overføringstjenester. Dessverre er Googles sikkerhetskopieringsalternativer - Nærlinje-sikkerhetskopiering for ofte tilgjengelige data og Coldline-sikkerhetskopiering for sjelden tilgjengelige data - også ganske grunnleggende.

Flere fremragende funksjoner fra GCP inkluderer:

- høy grad av skalerbarhet
- enkel konfigurasjon og installasjon

- bruk av mye brukte programmeringsspråk som Python og Java
- Rimelige langsiktige besparelser
- Databelastningsbalansering og raske svar.

Ulemper inkluderer følgende:

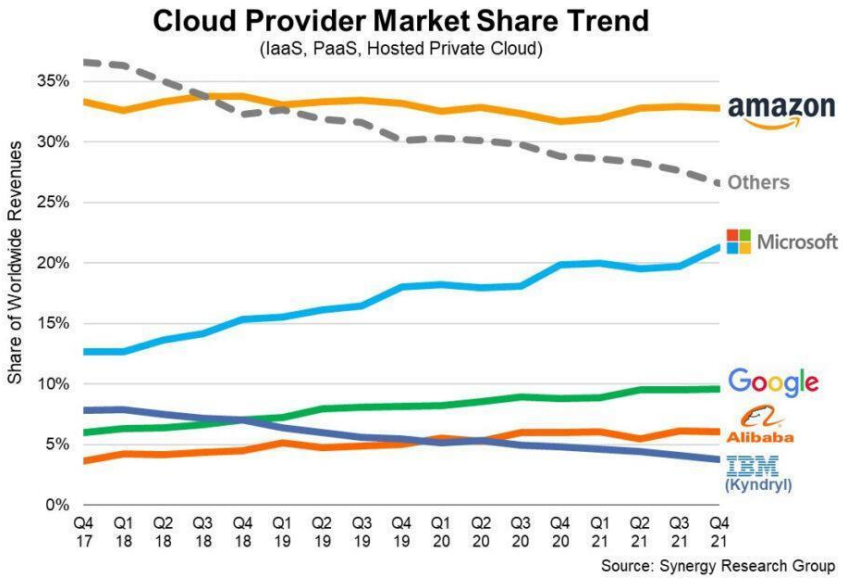
- Utilstrekkelige avanserte funksjoner
- Mindre variasjon i funksjoner
- Færre servicealternativer
- Det er færre globale datasentre.

Spørsmål å vurdere

- Hva er en skyplattform, og hvilke fordeler gir den?
- Navn 3 av bedriftens fordeler fra skyen i grafen og hvorfor de appellerer til deg.
- Hvem ville du valgt som leverandør og hvorfor?
- Sjekk kilden, med tittelen Techfunnel (2022) og svar med det du har lært.

2.2.2 De 3 sentrale aktørene på markedet

Tre store skytjenesteleverandører kontrollerer majoriteten av markedet i 2021, og står for 64% av den totale markedsandelen. Som vist i diagrammet nedenfor, har AWS topplasseringen med en markedsandel på 33%, tett fulgt av Azure med 21% og Google Cloud med 10%, som vist i figuren (diagrammet) nedenfor.



Figur 2.5. Skyleverandør Markedsdel Trend

På grunn av disse skyleverandørenes omfattende globale nettverk, kan disse tallene forklares. Med et marked som bare blir større, er Amazon et interessant tilfelle fordi markedsandelen har stabilisert seg på rundt 33%. Med andre ord, de siste årene har AWS-skyinntektene økt jevnt og trutt. Selv om konkurransen blir sterkere, har AWS solgt sine skyprodukter i 11 år og fortsetter å være markedsleder. Andre etterligner hva Amazon gjør når det vedtar en ny teknologi eller forretningsstrategi.

Ifølge Jeff Bezos, tidligere administrerende direktør i Amazon, "hadde AWS den uvanlige fordelen av et syvårs forsprang før de møtte likesinnet konkurranse." På grunn av dette er AWS-tjenester langt de mest avanserte og funksjonelle. AWS rapporterte en omsetning på 62 milliarder dollar og et nettoresultat på 18.5 milliarder dollar i 2021. Sammenlignet med fjorårets omsetning representerer det en økning på 38 prosent.

Microsoft er utvilsomt AWS største konkurrent; Intelligent Cloud Division of Microsoft genererte 60 milliarder dollar i inntekter i fjor, noe som er svært nær AWS inntekter, men her er haken: denne divisjonen inkluderer også mange andre tjenester, inkludert Microsoft Azure, GitHub, Windows Server, Microsoft SQL Server og andre versjoner av disse produktene. Den intelligente skydivisjonens inntekter økte med 24 % fra 2020 til 2021.

Google Cloud er den tredje største skyleverandøren etter AWS og Azure.

Inntektene vokste fra 13 milliarder dollar i 2020 til 19 milliarder dollar i 2021. Driftsunderskuddet i Google Cloud gikk ned 2,5 milliarder dollar fra 2020 til 2021. Nedgangen i driftsunderskudd var hovedsakelig drevet av vekst i inntektene.

I likhet med Microsoft Azure inneholder Googles skydivisjon også tilbakemeldinger fra andre steder, for eksempel Google Workspace. De foregående årene så betydelige investeringer gjort av Google Cloud, noe som resulterte i driftstap, for å ta igjen AWS og Azure. Tidligere i 2022 spådde Ruth Porat, finansdirektør i Google og Alphabet, dette på følgende måte: "Når vi ser fremover, vil vi fortsette å fokusere på inntektsvekst drevet av pågående investeringer i produkter og go-to-market-organisasjonen ... Skala vil etter hvert redusere driftstapet og forbedre driftsmarginen.

Her er en rask titt på noen viktige aspekter ved hver:
Azure Virtual Network: Azure er for øyeblikket tilgjengelig i 54 områder over hele verden og holder så mye trafikk som mulig inne i Azure-nettverket i stedet for over Internett. Til slutt er det en nettverksløsning som yter bedre enn selv AWS er rask og sikker. I tillegg, fordi Azure Virtual Network er så fleksibelt, kan bedrifter bruke en hybrid nettverksstrategi eller ta med sine egne IP-adresser og DNS-servere.

Amazon Direct Connect: For å garantere konsistent tjeneste og pålitelig ytelse til enhver tid, har Amazon skapt et omfattende globalt rammeverk sentrert rundt 114 kant-lokasjoner, 14 datasentre og 22 forskjellige globale

regioner. Som et resultat er AWS i stand til å tilby raske skydistribusjonsmodeller, rask levering og øyeblikkelige responstider for sitt brede spekter av tjenester. Spesielt 802.1q VLAN-ene, som er industristandarder, muliggjør en dedikert forbindelse mellom private nettverk og AWS via noen av de mange Direct Connect-stedene.

GCP: Til tross for at Google ikke har samme omfang som de to andre leverandørene, støtter Googles anerkjente innovasjonsfunksjoner Google Cloud Platform. I tillegg til et stort antall datasentre over hele verden, har Google for tiden 21 regioner og legger kontinuerlig til flere med tillegg av undersjøisk kabling. Hybride tilkoblingsprodukter som Cloud Interconnect og Cloud VPN gjør det mulig å opprette sikre direktetilkoblinger eller IPsec VPN-tilkoblinger.

For å forstå skymarkedsandelen for hver av de tre store leverandørene, bør du også være kjent med hvert selskaps nåværende aksjetall:
AWS: Med en markedsandel på 32% totalt, styrer Amazon det globale markedet. Det overgikk faktisk de to andre mest populære skyplattformene når det gjelder inntekter, og brakte inn respektable 11.6 milliarder dollar og opplevde en vekstrate på 29% dette kvartalet.

Azure: Med Azure, som har en markedsandel på 19 %, har Microsoft en betydelig markedsandel. Microsoft rapporterte en vekstrate på 48 % i forhold til forrige kvartal, til tross for at de ikke offentliggjør Azures inntektstall.

Google Cloud Platform: GCP vokser fortsatt raskt og ligger for øyeblikket på tredjeplass med en markedsandel på 7 %. Veksten er faktisk 45% året over, med 3, 44 milliarder dollar i totale inntekter dette kvartalet.

Etter pandemien som akselererte implementering av cloud computing de siste to årene, kan vi se at tallene fortsetter å stige og at krisen var mer en langsiktig booster for skymarkedet enn en kortsiktig effekt.

Det ble nylig bemerket at bedrifter som omfavnet cloud computing de siste årene har økt bruken og beveger seg nå mer og mer mot multi cloud strategier. Flexera State of the Cloud 2022-rapporten har også vist at bedrifter investerer en økende sum penger i disse teknologiene, og at nye problemer som sikkerhet, multi cloud-administrasjon og Kubernetes-adopsjon dukker opp som et resultat. Siden innsatsen alltid er høyere, er det avgjørende for bedrifter å bedre forstå og utnytte ressursene så effektivt som mulig.

Selskaper gjør betydelige investeringer på global skala. Utgiftene til offentlige skyer vil øke fra 408 milliarder dollar i 2021 til 474 milliarder dollar innen utgangen av 2022, ifølge Gartners prognose.

Spørsmål å vurdere

- Hva er de nåværende markedsandelsprosentene blant leverandørene?

- Ta hensyn til forskjellene mellom tilbydere i skymarkedsandel.
- Hvorfor vil markedsandelen øke eller redusere: nevn noen faktorer og angi hva noen av dine fremtidige spådommer kan være for de 3 leverandørene.

2.2.3 Sammenligning av markedsandeler i skyen

For bedre å forstå hvordan markedet klarer seg globalt, la oss se på globale markedsandeler holdt av de store 3 i følgende store markeder: i USA, i Europa og i Kina.

Det amerikanske skymarkedet
Det bør ikke være overraskende at det amerikanske skymarkedet, som står for 44% av alle globale utgifter, er det desidert største. De tre største skytjenesteleverandørene har fortsatt samme markedsandel: AWS har 37 %, Azure har 23 % og GCP har 9 %. AWS, Azure og Google Cloud åpnet nye datasentre i USA i 2021. Microsoft Azure, for eksempel, begynte å operere i Georgia og Arizona i 2021, og dette tallet vil fortsette å øke ettersom de nylig kunngjorde planer om å bygge 50 til 100 nye datasentre hvert år over hele verden. Fra figuren nedenfor kan vi se kostnadene for skyinfrastrukturtjenester for Q1 2021 sammenlignet med årene 2019 og 2020.

Figur 2.6. Kostnadene for skyinfrastrukturtjenester for Q1 2021 i USA sammenlignet med år 2019 og 2020

Det amerikanske skymarkedet er det desidert største og står for 44% av de totale utgiftene, noe som ikke er overraskende. På grafen ovenfor kan du se betydelige veksttopper (38%) under COVID-krisen og mer nylig, en vekst på 29% i Q1 2021 for å nå en rekord på $18,6B.

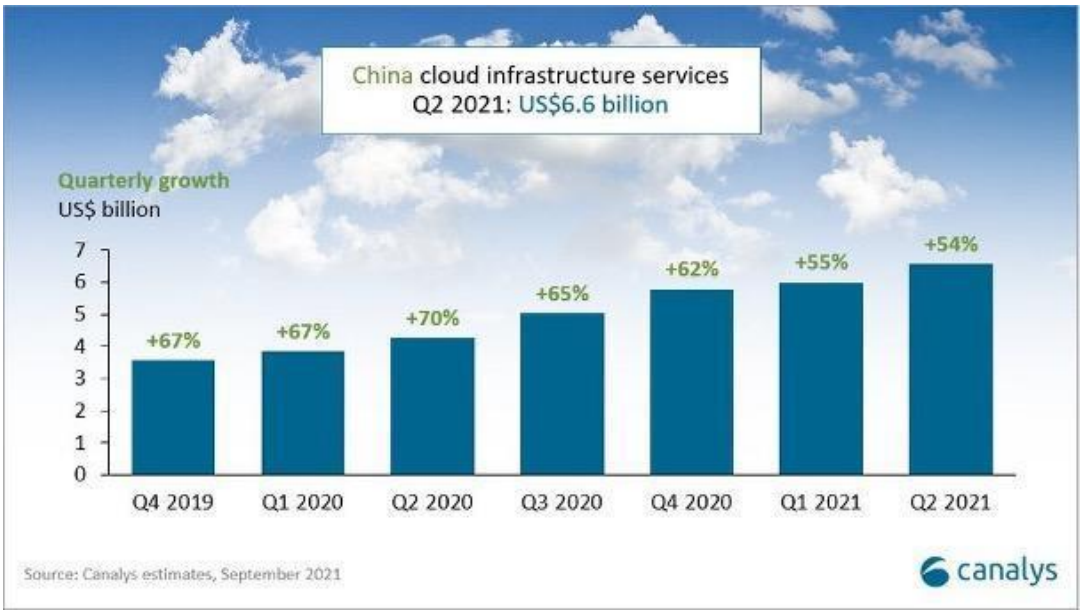
Skymarkedet i Europa
Selv om det har økt i løpet av Covid-tiden, er det europeiske skymarkedet fortsatt bare det tredje største etter USA og Kina.

Nasjonale skytjenesteleverandører som Deutsche Telekom, OVH, Scaleway, Orange og ulike nasjonale telekomselskaper er tilgjengelige i det europeiske markedet. Disse leverandørene konkurrerer med de tre største skytjenesteleverandørene i verden, AWS, Azure og GCP, som nå kontrollerer 66 % av markedet, opp fra 50 % for tre år siden.

Det europeiske skymarkedet forventes å vokse veldig sterkt i de kommende årene, med nye datasentre som dukker opp over hele kontinentet, til tross for dets treghet i forhold til andre viktige regioner. I 2030, ifølge ulike prognoser, vil det europeiske markedet være verdt mer enn 300 milliarder dollar, noe som vil være lik størrelsen på det globale markedet i dag.

Skymarkedet i Kina

Det kinesiske skymarkedet vokser fortsatt dobbelt så raskt som i USA (60 vs. 30%), og overgår resten av verden. Kina utgjorde 14% av det globale skymarkedet i Q2 2021, med utgifter til skyinfrastruktur som oversteg 6 milliarder dollar, som vist i figuren (diagrammet) nedenfor.



Figur 2.7. Kostnadene for skyinfrastrukturtjenester for Q1 2021 i Kina sammenlignet med år 2019 og 2020

Pandemien har akselerert veksten på samme måte som den har gjort i andre markedsregioner; kvartal 2020 nådde veksten en topp på 70 %. Det er andre underliggende årsaker til denne raske veksten: Kina er den eneste betydelige økonomien som rapporterte økonomisk vekst for 2020, med en BNP-vekst på 2,6 %. Den kinesiske regjeringen har gjort cloud computing en topp prioritet gjennom sin "internett pluss"-strategi i 2015.

Regjeringen fremmer og subsidierer skybransjen. Kinesiske teknologigiganter som Alibaba, Tencent, Baidu, Huawei tilbyr skyløsninger og kan konkurrere mot sine amerikanske rivaler ettersom de har en tilsvarende

størrelse. Alibaba, Huawei Cloud, Tencent og Baidu AI Cloud, som til sammen står for mer enn 80% av de totale utgiftene, er de primære skyleverandørene i det kinesiske skymarkedet. Amerikanske selskaper sliter på grunn av lover som favoriserer kinesiske bedrifter.

Kinesiske skytjenesteleverandører tar nå sikte på å vokse i Europa, Asia og utviklingsland. Vi kan forvente en digital konkurranse mellom USA og Kina, tilsvarende 5G-nettet.

Spørsmål å vurdere

- Hva er nøkkelstatistikken til US Cloud-markedet?
- Hvor mye forventes det globale markedet å være verdt i Europa innen 2030?
- Nevn to måter Kina kan håpe å utfordre det amerikanske markedet på, og spår du at de vil lykkes med sine ambisjoner?

2.2.4 Analyse av prisstrukturer

For å forstå prisstrukturer er det viktig å vite at hver av de tre hovedplattformene har to ting til felles: et gratis nivå med svært få alternativer og en prismodell per time eller minutt på forespørsel for alle ressurser. Sammenligning av priser kan være utfordrende fordi de kan variere betydelig avhengig av ressursbruk, tjenestepreferanser og andre faktorer.

Generelt er en priskrig alltid i spill blant de tre beste: Ved å senke prisene, forsøker Microsoft og Google å utfordre AWS. Brukere av AWS-tjenester betaler kun for det de bruker, uten ekstra gebyrer eller oppsigelsesgebyrer etter at tjenesten er fullført. Dette er kjent som en pay-as-you-go-modell.

Her er hovedtrekkene i prismodellene til alle tre leverandørene:

Priser for AWS. Det har blitt uttalt at prisstrukturen levert av Amazon er "så kompleks at du trenger en tredjepartsapp for å administrere den." Amazon tilbyr imidlertid en 12-måneders periode på 750 timer per måned med EC2-tjenester som en del av gratisnivået, samt opptil 75% rabatt for en forpliktelse på 1–3 år.

- Høy pris i sammenligning
- Tilleggskostnader for nødvendige tjenester
- Kostnader for teknisk kundestøtte belastes i tillegg.

Prisstrukturen i AWS er så kompleks at du trenger en tredjepartsapp for å administrere alle disse tjenestene. Den minste instansen, som har 2 virtuelle CPUer og 8 GB RAM, vil koste deg omtrent USD 69 per måned, mens den største instansen, som har 128 virtuelle CPUer og 3.84 TB RAM, vil koste deg omtrent USD 3.97 per time.

Azure-priser. Azure-brukere bruker ofte en tredjepartsapp til å administrere kostnader fordi den er kompleks på en måte som ligner på AWS. I likhet med AWS tilbyr Azure et gratisnivå som lar brukere bruke 750 timer med virtuelle maskiner per måned i 12 måneder i bytte mot en kraftig rabatt hvis de forplikter seg til en periode på ett til tre år.

- Rabatter på tjenesteavtaler for brukere av Microsofts cloud computing-tjenester
- Rimelige priser på forespørsel
- Bruk av høye redundans for å redusere nedetid.

En rekke variabler, inkludert plassering, nødvendig kapasitet og administrasjonsnivå, påvirker prisen på Azure. Det tilbyr også et gratis nivå, som tillater gratis bruk av noen modeller bare de første 12 månedene, samt gratis bruk av noen modeller for alltid.

Forbruksbetalte priser er et alternativ med Azure, akkurat som med AWS. Det tilbyr også en annen måte å forhåndsbetale for tjenesten på, som den refererer til som "reservert instans" (forhåndsforpliktelse). I tillegg gir den spot-instanser, slik at kunder kan kjøpe virtuelle maskiner (VM-er) fra Azures overflødige kapasitet til en rabatt.

Brukere kan starte eller stoppe tjenesten etter behov og bare betale for sekundene de faktisk bruker når de bruker pay-as-you-go-metoden. Den reserverte instansen er derimot designet for kontinuerlig bruk og er basert på kostnaden for en hel måned (730 timer), mens pay-as-you-go-modellen også er avhengig av 730-timersanalysen, ifølge priskalkulatoren. Microsoft Azure tillater et bredt spekter av tjenester som databehandling, nettverk, lagring og analyse. Derfor avhenger prismodellen av ulike faktorer, inkludert nødvendig kapasitet, plassering, type tjeneste og administrasjonsnivå.

Google-priser. Det er tydelig at Google gjorde en innsats for å lære av feilene til sine rivaler og vedtok en kostnad per sekund-modell som er ganske enkel. I tillegg tilbyr GCP USD 300 i kreditt for ett års tjeneste, én gratis mikro-instans per måned det første året av gratisnivået og 30 % rabatt for fortsatt bruk.

De tilbyr en rekke prisalternativer, for eksempel pay-as-you-go-priser, langsiktige reservasjoner og gratis nivåalternativer. Kostnaden for Google Cloud påvirkes også av en rekke faktorer, inkludert priser for databehandling, SQL, nettverk, lagring og serverløs. Du bør vurdere disse faktorene når du velger en kostnadsstruktur for en bedrift.

Google tilbyr sine kunder USD 300 kreditt gratis som kundene kan bruke beløpet på Google Cloud-produktene sine. Brukere kan også benytte seg av en rekke gratis produkter, inkludert de mest populære skytjenestene som for øyeblikket er tilgjengelige på markedet for databehandling, lagring, databaser, IoT og kunstig intelligens. I tillegg tilbyr den amerikanske teknologigiganten betydelige rabatter for produkter som er "forpliktet til bruk", eller brukt på et bestemt nivå i ett eller tre år i forveien.

Google tilbyr sine brukere et spesielt valg kjent som "Vedvarende bruksrabatter." Hvis du bruker tjenestene i en viss prosentandel av måneden, vil dette tilbudet automatisk bli brukt på en glidende skala. I tillegg er du ikke pålagt å foreta forskuddsbetalinger eller signere noen forpliktelser for å kombinere ikke-overlappende instanser og motta fordelene med en prosentvis rabatt opp til maksimumsnivået.

Her er et diagram som viser prissammenligningene mellom plattformene:

AWS Vs. Azure Vs. GCP Cloud Cost Comparison

Detail	Amazon AWS	Microsoft Azure	Google GCP
Minimum Instance	2 virtual CPUs, and 8 GB of Ram will price you around – USD 69/month	2 virtual CPUs, and 8 GB of Ram will price you around – USD 70/month	2 virtual CPUs, and 8 GB of Ram will price you around – USD 52/month
Maximum Instance	3.84 TB Ram, 128 vCPUs will price you around – USD 3.97/hour	3.89 TB Ram, 128 v CPUs will price you around – USD 6.97/hour	3.75 TB Ram, 160 v CPUs will price you around – USD 5.32/hour
Type of Discount	Reserved Instances (RIs)	Reserved Instances (RIs)	Committed Use Discount (CUD) Sustained Use Discount (SUD)
Commitment	1 or 3 years	1 or 3 years	Committed Use Discount (CUD) – 1 or 3 years Sustained Use Discount (SUD) – no commitment
Discount percentage	Up to 75 percent	Up to 72 percent	Committed Use Discount (CUD) – for 1 year up to 37 percent or 3 years up to 55 percent Sustained Use Discount (SUD) – up to 30 percent
Is cancellation available?	Yes, it offers to sell your products on the marketplace	Yes, they will charge a 12% cancellation fee	No cancellation is available
Payment options	3 options are available on AWS – no up-front, partial up-front, all up-front	All up-front	No up-front
High Profile Customers	LinkedIn, Facebook, BBC, Airbnb, Twitch, Netflix, Adobe, ESPN, Lamborghini, etc.	Apple, HP, Coca-Cola, LG Electronics, Verizon, Xbox, Fujifilm, etc.	Twitter, Intel, Yahoo, PayPal, eBay, Target, 20th Century Fox, etc.

Figur 2.8. Sammenligning av AWS kontra Azure kontra GCP-skykostnader

Spørsmål å vurdere

- Hva er den mest tiltalende prisstrukturen for deg og hvorfor?
- Hvorfor er det vanskelig å foreta en direkte prissammenligning blant konkurrentene?
- Nevn de to aspektene alle 3 konkurrentene deler, og vurder hvordan du kan selge plattformene basert på forskjellene mellom dem.

2.3 Velge og angi infrastrukturen

2.3.1 Distribuere servere og belastningsfordelere på alle databehandlingsplattformer

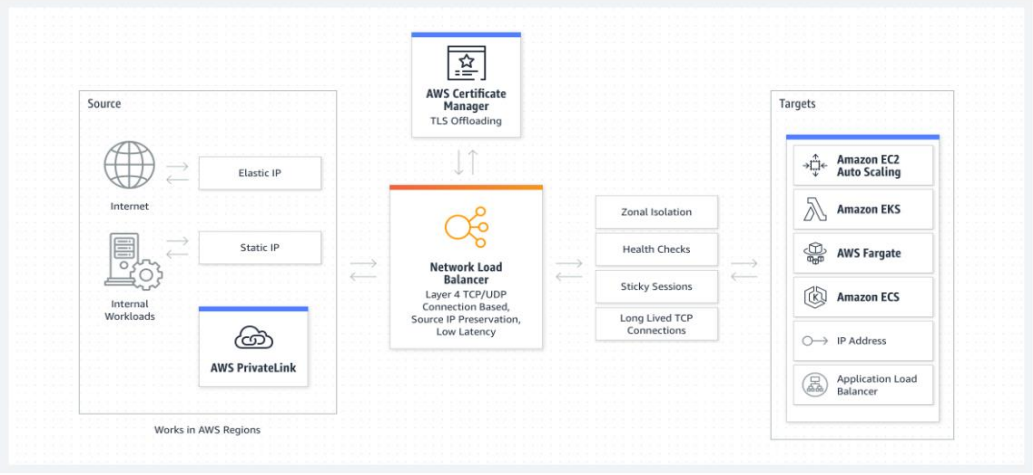
I denne enheten vil vi se på rollene til lastbalansering, som er en metode for å hjelpe et nettverk med å unngå irriterende nedetid og levere optimal ytelse til brukere ved å behandle oppgaver og dirigere økter på forskjellige servere. Dette gjøres forskjellig i forskjellige skynettverk. I denne enheten vil vi se på de viktigste 3: AWS, Azure og Google Cloud Services.

Hva er en lastbalanserer?
En lastbalanserer deler brukertrafikk mellom flere instanser av programmene dine. Lastbalansering reduserer sannsynligheten for ytelsesproblemer i programmene dine ved å spre belastningen. Cloud Load Balancing er en programvaredefinert, fullt distribuert administrert tjeneste. Fordi det ikke er maskinvarebasert, er du ikke pålagt å administrere en fysisk infrastruktur for lastbalansering.

Lastbalanserere klassifiseres i henhold til plattformen deres, og her vil vi sammenligne plattformene med noen av deres nøkkellastbalanserere og grafer som illustrerer casene:
Amazon Web Tjenester (AWS)
Elastic Load Balancing (ELB) distribuerer innkommende programtrafikk på tvers av flere mål og virtuelle apparater i én eller flere tilgjengelighetssoner automatisk (AZ-er). En applikasjonslastbalansering tar beslutninger om ruting i applikasjonslaget(HTTP/HTTPS), støtter banebasert ruting og kan rute forespørsler til én eller flere porter på hver beholderinstans i klyngen. Dynamisk tilordning av vertsport støttes av applikasjonsbelastningsfordelere. Nedenfor er en figur (graf) som beskriver Application Load Balancer for AWS.

Figur 2.9. Applikasjonslastbalansering for AWS

En nettverkslastbalansering tar rutingsbeslutninger på transportlaget (TCP/SSL). Den kan behandle millioner av forespørsler per sekund. Når en tilkobling mottas, bruker lastbalanseringen en flythash-rutingalgoritme til å velge et mål fra målgruppen for standardregelen. Den prøver å opprette en TCP-tilkobling til det valgte målet på porten som er angitt i lyttekonfigurasjonen. Den sender forespørselen med meldingshodene uendret. Når lastbalansereren mottar en tilkobling, bruker den en rutingalgoritme for flythash til å velge et mål fra målgruppen for standardregelen. Forespørsler blir sett på som om de kommer fra den private IP-adressen til nettverkslastbalanseringen når de er konfigurert med IP-adresser som mål. Dette betyr at når du tillater innkommende forespørsler og tilstandskontroller i målets sikkerhetsgruppe, er tjenester bak en Network Load Balancer effektivt åpne for verden (som vist fra figuren nedenfor).

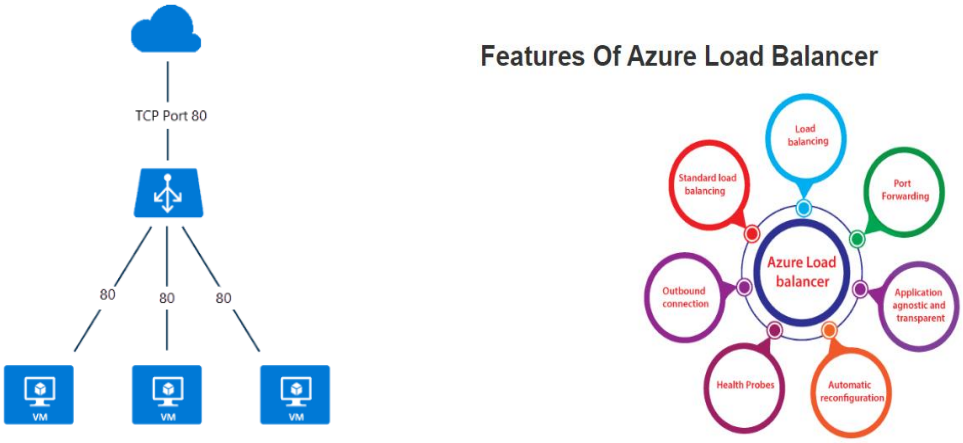


Figur 2.10. Lastbalansering for nettverk

Azure

En Azure-lastbalanserer brukes til å distribuere trafikkbelastninger til virtuelle maskiner eller skaleringssett for virtuelle maskiner. Du kan bruke en lastbalanserer mer fleksibelt ved å definere dine egne lastbalanseringsregler. Prosessen med jevnt fordelt belastning (innkommende nettverkstrafikk) på tvers av en gruppe backend-ressurser eller servere kalles lastbalansering. Du kan bruke Azure lastbalansering til å distribuere trafikk til virtuelle maskiner på serverdelen. En Azure-lastbalansering sikrer at programmet ditt alltid er tilgjengelig. Azure-lastbalanseringen er en selvadministrert tjeneste.

Utgående tilkoblinger for virtuelle maskiner (VM-er) i det virtuelle nettverket kan leveres av en offentlig lastbalansering. Disse tilkoblingene er mulig ved å konvertere private IP-adresser til offentlige IP-adresser. Public Load Balancers brukes til å levere balansert internettrafikk til dine virtuelle maskiner. Når bare private IP-adresser kreves i frontend, brukes en intern (eller privat) lastbalansering. Interne lastbalanseringer bidrar til å balansere trafikken i et virtuelt nettverk. I et hybridscenario kan du få tilgang til en frontend for lastbalansering via et lokalt nettverk. Lastbalansereren er presentert nedenfor i figur 2.11.



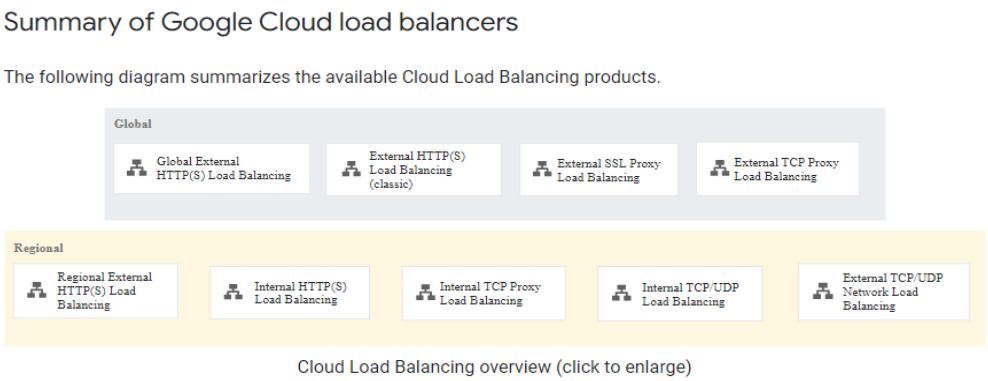
Figur 2.11. Lastbalanserere

Noen av de viktigste scenarioene som en Azure gjør gjennom en Standard Load Balancer inkluderer:

- Direkte intern og ekstern trafikk til virtuelle Azure-maskiner,
- Fordel ressurser innenfor og på tvers av soner for å øke tilgjengeligheten,
- Overvåk belastningsbalanserte ressurser med tilstandssonder,
- Gjennom Azure Monitor, gir flerdimensjonale måledata.

GCS Cloud Load Balancing er bygget på den samme infrastrukturen som driver Googles frontend. Den kan håndtere 1 million eller flere spørringer per sekund samtidig som den opprettholder konsekvent høy ytelse og lav ventetid. Cloud Load Balancing-trafikk går inn gjennom 80+ forskjellige globale lastbalanseringssteder,

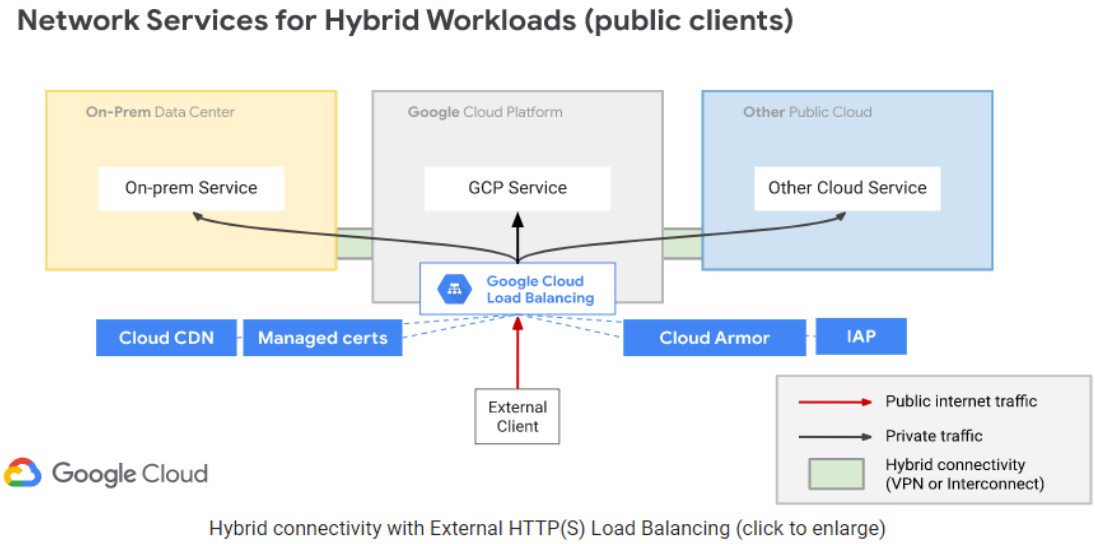
og maksimerer avstanden som er reist på Googles raske private nettverksryggrad. Du kan vise innhold så nær brukerne som mulig ved å bruke Cloud Load Balancing (figur 2.12. nedenfor).



Figur 2.12. Velge en Cloud Load Balancer

Hvis du vil velge et produkt for lastbalansering i skyen, må du først bestemme hvilken type trafikk lastbalanserere må håndtere, samt om du trenger global eller regional lastbalansering, ekstern eller intern lastbalansering og proxy- eller gjennomgangsbelastningsbalansering. Lastbalansering i skyen kan lastbalansere trafikk til andre endepunkter enn Google Cloud, lokale datasentre og andre offentlige skyer som er tilgjengelige via hybridtilkobling.

Figuren (diagrammet) nedenfor viser en hybriddistribusjon med en ekstern global HTTP(S)-lastbalansering.

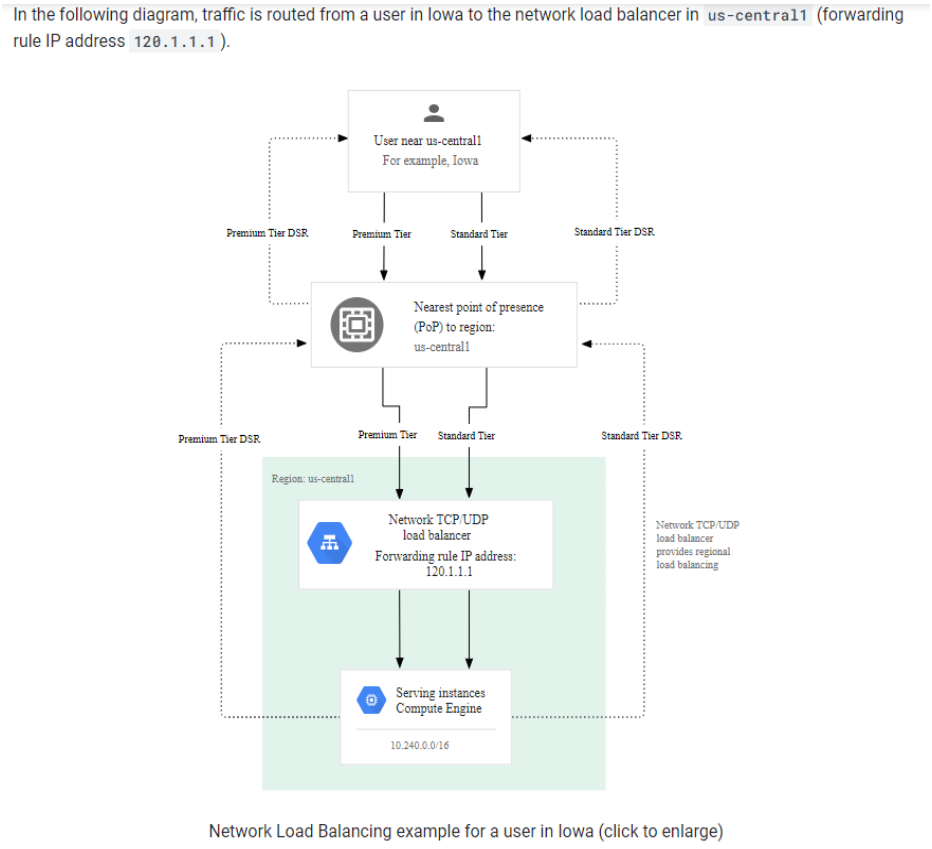


Figur 2.13. Hybriddistribusjon med en ekstern global HTTP(S)-lastbalansering

En GCS-nettverkslastbalansering kan godta trafikk fra

- hvilken som helst internettklient.
- Virtuelle Google Cloud-maskiner med eksterne IP-adresser
- Virtuelle Google Cloud-maskiner som har Internett-tilgang via Cloud NAT eller instansbasert NAT
- Følgende er egenskapene til nettverkslastbalansering i GCS:
- En administrert tjeneste er lastbalansering i nettverket.
- Andromeda virtuelt nettverk og Google Maglev brukes til å implementere nettverksbelastningsbalansering.
- Lastbalanseringer på nettverk er ikke proxyer.
- Virtuelle serverdel-maskiner mottar belastningsbalanserte pakker med kilde- og mål-IP-adresser, protokoll og, hvis protokollen er portbasert, kilde- og målportene uendret.
- De virtuelle serverdel-maskinene avslutter belastningsbalanserte tilkoblinger.

Nedenfor finner du et eksempel på en Network Load Balancer i et brukertilfelle:



Figur 2.14. Network Load Balancer i et brukertilfelle

Spørsmål å vurdere:

1. Hvorfor bør du bruke en lastbalanserer?
2. Nevn en funksjon som er nyttig fra hver skyplattform å vurdere
3. Fyll ut de tomme feltene i denne erklæringen: Cloud Load Balancing er en ____ Fordi det ikke er ____, er du ikke pålagt å administrere en fysisk infrastruktur for lastbalansering.
4. Nevn to av de viktigste scenariene som en Azure gjør gjennom en Standard lastbalansering.

2.3.2 Lagringstjenester i skyen

Tre av de største skyleverandørene Amazon Web Services (AWS), Google Cloud Platform (GCP) og Microsoft Azure (Azure) tilbyr alle tre hovedtyper lagring på plattrformene sine. Objektlagring, også kjent som blob-lagring i Microsoft Azure, blokklagring og fillagring, hvor alle har sine fordeler og ulemper og forskjellige brukstilfeller.

For objekt-/bloblagring er de tre største tjenestene AWS sin Simple Storage Service (S3), Googles Cloud Storage og Microsofts Azure Blobs. Disse tre gjør stort sett de samme tingene, med noen variasjoner i retningslinjene og lagringsnivåene de tilbyr, og prisnivåene de har for lagring per GB og for tilgang til filene.

Alle tre leverandørene har minst tre generaliserte lagringsnivåer kategorisert i det som kalles aktiv, kjølig og kald lagring. Disse navnene angir hvor ofte dataene som oppbevares i lagringen, er blir benyttet.

Aktiv lagring er for data som vil bli brukt ofte og med så lav ventetid som mulig. Et eksempel på hva slags data som bør lagres i aktiv lagring, er produktbilder i en nettbutikk. Kunder ønsker å kunne se fotografier av varene i butikken med så lav ventetid som mulig, og trenger ikke å vente på at nettstedet skal hente og laste bildet i nettleseren.

Kjølig lagring er for data som bør nås sjelden. Et eksempel på kjølig lagring kan være en aggregert-salgsrapport. Dataene i rapporten brukes kanskje bare én gang i måneden for å oppdatere med data for forrige måned, ellers er tilgangen minimal. Det er mye billigere å lagre data i et kjølig lagringsnivå enn i aktive data, men kommer på bekostning av en mye høyere pris for tilgang til dataene, og med et minimum lagringstid.

S3 Standard lagringsnivå med en pris på nær dobbelt så mye som Infrequent Access som vist i figuren nedenfor.

S3 Standard - General purpose storage for any type of data, typically used for frequently accessed data	
First 50 TB / Month	$0.024 per GB
Next 450 TB / Month	$0.023 per GB
Over 500 TB / Month	$0.022 per GB

Figur 2.15. En prissammenligning mellom aktiv lagring og kjølig lagring med AWS S3

S3 Standard - Infrequent Access** - For long lived but infrequently accessed data that needs millisecond access	
All Storage / Month	$0.0131 per GB
S3 One Zone - Infrequent Access** - For re-createable infrequently accessed data that needs millisecond access	
All Storage / Month	$0.01048 per GB

Figur 2.16. Infrequent Access-priser

S3 Infrequent Access tilbyr en svært lav pris per GB.

Men S3-standardnivået tilbyr en mye lavere pris for å få tilgang til dataene som er lagret i beholderene.

	PUT, COPY, POST, LIST requests (per 1,000 requests)	GET, SELECT, and all other requests (per 1,000 requests)	Lifecycle Transition requests into (per 1,000 requests)	Data Retrieval requests (per 1,000 requests)	Data retrievals (per GB)
S3 Standard	$0.0053	$0.00042	n/a	n/a	n/a
S3 Standard - Infrequent Access **	$0.01	$0.001	$0.01	n/a	$0.01
S3 One Zone - Infrequent Access **	$0.01	$0.001	$0.01	n/a	$0.01

Figur 2.17. S3 Standard priser

Kald lagring brukes til data som svært sjelden blir benyttet, en eller to ganger per år. Det vanligste brukstilfellet er arkivdata som må arkiveres i flere år av regulatoriske årsaker, men gjenfinningshastighet er mindre av en faktor, med gjenfinningshastigheter fra flere minutter til 12 timer.

En type arkiv som avviker litt er visse helsedata der det svært sjelden er behov for tilgang, men når behovet oppstår må det være tilnærmet umiddelbar tilgang.

Kald lagring er den billigste av lagringstypene for selve dataoppbevaringen. Men de lave kostnadene ved lagring av dataene kommer på bekostning av en mye høyere pris for tilgang og gjenfinning av dataene.

S3 Glacier Instant Retrieval ***	$0.02	$0.01	$0.02	n/a	$0.03
S3 Glacier Flexible Retrieval ***	$0.0318	$0.00042	$0.0318	See below	See below
Expedited	n/a	n/a	n/a	$10.50	$0.0315
Standard	n/a	n/a	n/a	$0.053	$0.0105
Bulk ***	n/a	n/a	n/a	n/a	n/a
Provisioned Capacity Unit ****	n/a	n/a	n/a	n/a	$105.00 per unit
S3 Glacier Deep Archive ***	$0.06	$0.00042	$0.06	See below	See below
Standard	n/a	n/a	n/a	$0.106	$0.021
Bulk	n/a	n/a	n/a	$0.02625	$0.005

PUT, COPY, POST, LIST requests (per 1,000 requests)	GET, SELECT, and all other requests (per 1,000 requests)	Lifecycle Transition requests into (per 1,000 requests)	Data Retrieval requests (per 1,000 requests)	Data retrievals (per GB)

Figur 2.18. S3 Standard priser

Fra figur 2.19. under vises S3 Glacier Instant Retrieval, Flexible Retrieval og Deep Archive sammenligning av prisene.

S3 Glacier Instant Retrieval*** - For long-lived archive data accessed once a quarter with instant retrieval in milliseconds	
All Storage / Month	$0.005 per GB
S3 Glacier Flexible Retrieval (Formerly S3 Glacier)***- For long-term backups and archives with retrieval option from 1 minute to 12 hours	
All Storage / Month	$0.00405 per GB
S3 Glacier Deep Archive*** - For long-term data archiving that is accessed once or twice in a year and can be restored within 12 hours	
All Storage / Month	$0.0018 per GB

Figur 2.19. S3 Glacier Instant Retrieval, fleksibel gjenfinning og Deep Archive

Blokklagring: Amazon EBS, Azure Disks, Google Persisten Disk eller Local SSD

Blokklagring er en lagringstype der lagringsvolumene fungerer som lagringsstasjoner, omtrent som diskstasjonene på en fysisk bærbar eller stasjonær datamaskin.

Dataene lagres på disse stasjonene i blokker med data med fast størrelse. Disse blokkene får unike adresser slik at blokklagringsprogramvaren raskt kan finne plasseringen av dataene som trengs. Disse blokklagringsstasjonene kan også deles mellom flere forskjellige virtuelle maskiner og brukes ofte til lagring av data som trengs av applikasjoner som kjøres i mange forskjellige virtuelle maskiner.

En av fordelene med blokklagring sammenlignet med objektlagring er for data der store filer må endres og oppdateres ofte. Med en blokklagring trenger du bare å oppdatere blokkene der det er data som oppdateres, mens du i en objektlagring må oppdatere hele filen hver gang en endring gjøres.

Et annet brukstilfelle for blokklagring er som vedvarende lagring for applikasjoner som kjører på virtuelle maskiner. Hvis en virtuell maskin bare brukte den lokale lagringen som var tildelt den bestemte virtuelle maskinen, ville alle dataene den ville skrive, gå tapt når VM-en måtte starte på nytt, siden du aldri ville ha noen garanti for at serveren som kjører en bestemt instans av en virtuell maskin, vil være den samme neste gang VM-instansen kjøres. Dermed ville alle data skrevet ha gått tapt.

Når du velger klasse / lagringsnivå, er det viktig å ikke bare vurdere prisen, men også ting som tilgjengeligheten av tjenesten, hva slags tilgangsmønstre vil bli brukt (vil dataene bli brukt flere ganger i timen eller en gang i måneden, aktiv, kald?) Hvor lenge må dataene lagres?

For eksempel har AWS S3 Intelligent Tier som overvåker tilgangsmønstrene til dataene dine og beveger seg mellom S3-standarden og S3 Infrequent Access-nivåene for å redusere lagringskostnadene, noe som er en utmerket løsning hvis tilgangsmønsteret eller dataene dine ikke er fullt kjent.

En annen vurdering vil være hvilken leverandør som brukes i resten av virksomheten, og kjennskapen til medarbeidere i leverandørøkosystemet.

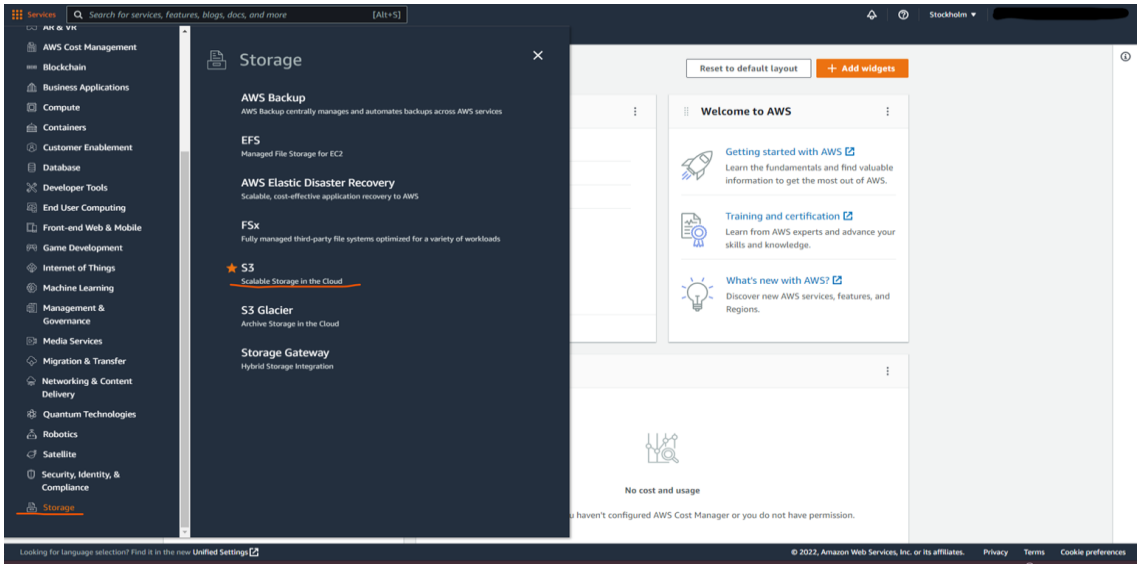
Ulike leverandører har også datasentre i forskjellige deler av verden, så det bør tas hensyn til hvilke regioner som er tilgjengelige med hvilke tjenester. Hvis du har lagringsplassen distribuert i områder så nær brukerne som mulig, reduseres ventetiden for tilgang til filene som er lagret.

Dette er alle hensyn som må tas når du velger hvilken lagringstype, og hvilket lagringsnivå, som passer best for dataene du har, og hvilken leverandør som tilbyr den beste generelle løsningen for dine spesielle forretningsbehov.

Per nå tilbyr Amazon 27 forskjellige regioner, med Microsoft Azure som har flest regioner med 42. Google kommer inn på 34 regioner.

Hvordan lage en beholder ved hjelp av Amazon AWS-konsollen:
Når du er på konsollens hjemmeside, klikker du på ikonet øverst til venstre som sier "Tjenester". Dette vil opprette en rullegardinmeny med en liste over AWS-tjenester. Rull ned til bunnen og klikk på 'Lagring'.

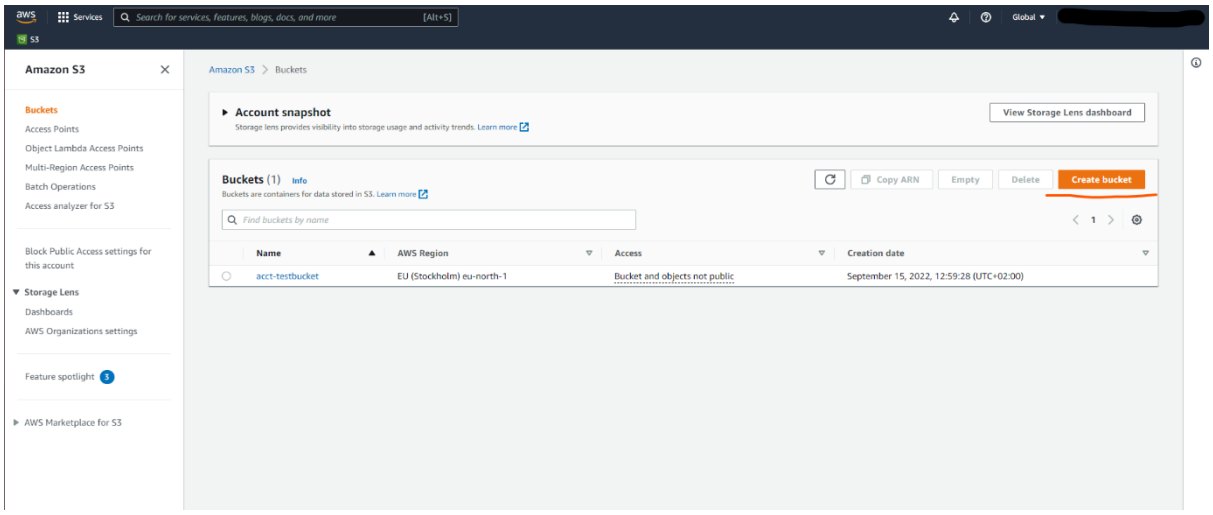
Dette åpner et sidepanel som viser de forskjellige lagringstjenestene som tilbys av AWS. Klikk på 'S3'. Dette tar deg til Amazon S3-konsollen.



Figur 2.20. S3-konsoll

Når du er i S3-konsollen, får du en liste over alle S3-beholderne på kontoen din (som vist i figur 2.20. ovenfor). Hvis dette er første gang du har åpnet S3-konsollen, vil det ikke listes noen beholdere.

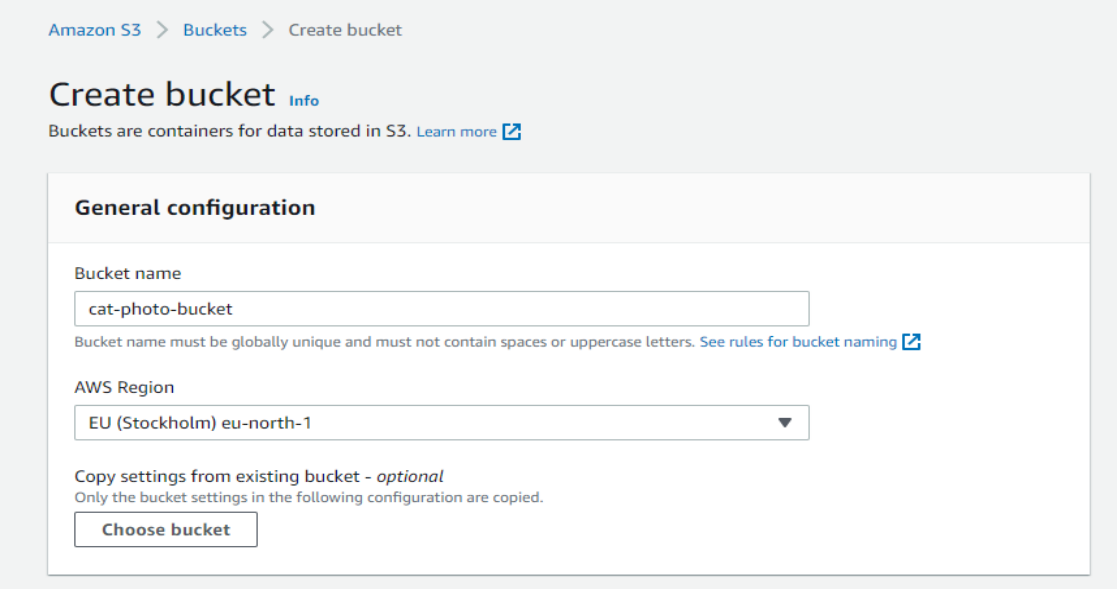
Klikk på den oransje knappen til høyre som sier "Create bucket" (som vist på figuren nedenfor).



Figur 2.21. Lag beholder i S3-konsollen

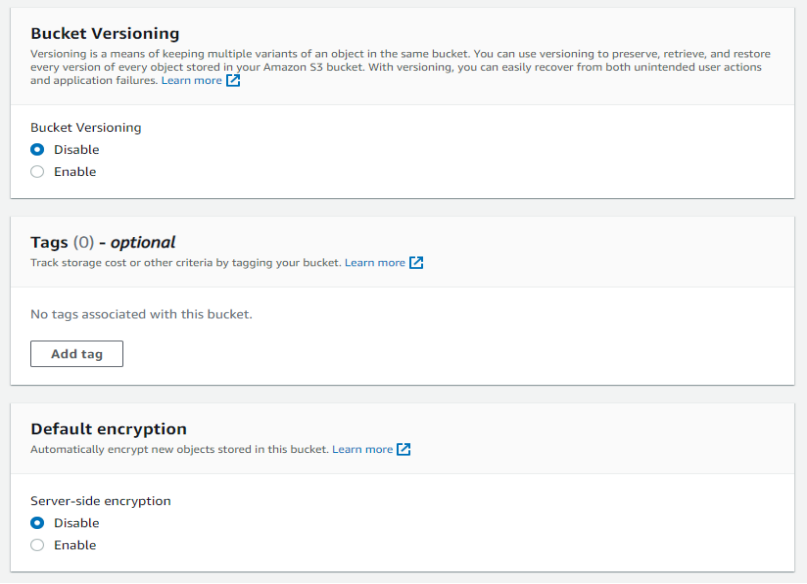
Når du har klikket på knappen, vil du bli presentert med "opprett beholder veiviseren".

Her vil du angi konfigurasjonen for beholderen (se figuren nedenfor). Disse inkluderer det globalt unike navnet på beholderen. Og AWS-regionen beholderen vil bli lagret i.



Figur 2.22. Opprett en beholder i S3-konsollen

Det er viktig å angi riktig region, da det å sette en beholder i et område som er langt borte fra brukerbasen din, kan introdusere ventetid for å få tilgang til filene som er lagret i beholderen.

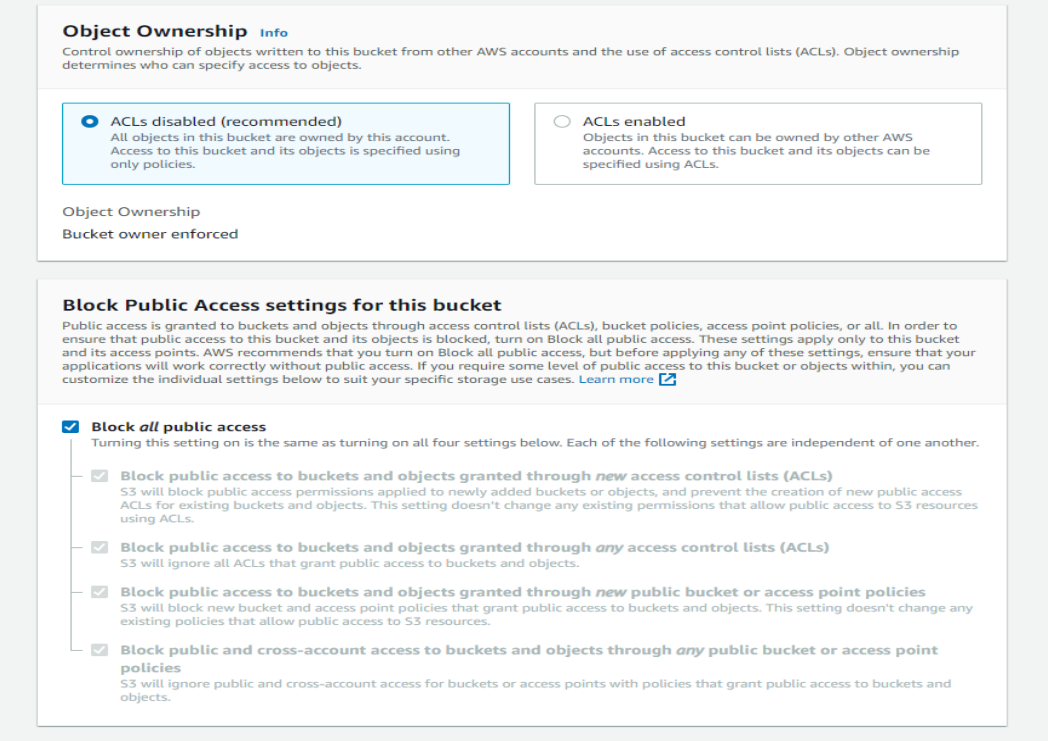


*Figur 2.23. Beholder*versjonering i S3-konsollen

Beholderversjonering (se figuren ovenfor) brukes til å holde et arkiv over alle de forskjellige iterasjonene av objektene i beholderen. Ved hjelp av versjonskontroll kan du føre en logg over endringer og redigeringer i samlingen, og du kan også rulle tilbake eller hente objekter i tilfelle det oppstår en feil, for eksempel en utilsiktet sletting.

Tagger kan brukes til å gi samlingene dine en enkel måte å gruppere beholdere sammen, slik at de kan brukes til f.eks. kostnadsfordeling, slik at kostnadene knyttet til et bestemt prosjekt spores riktig.

Standardkryptering lar deg bestemme om du vil at objektene i beholderen skal krypteres før AWS lagrer den i beholderen, slik at den forblir kryptert mens den er i ro, og bare dekrypterer den når den blir lastet ned igjen. Aktivering av kryptering krever at du konfigurerer en nøkkel for kryptering og dekryptering av objektene ved hjelp av enten Amazon S3-administrerte nøkler (SSE-S3) eller AWS Key Management Service.

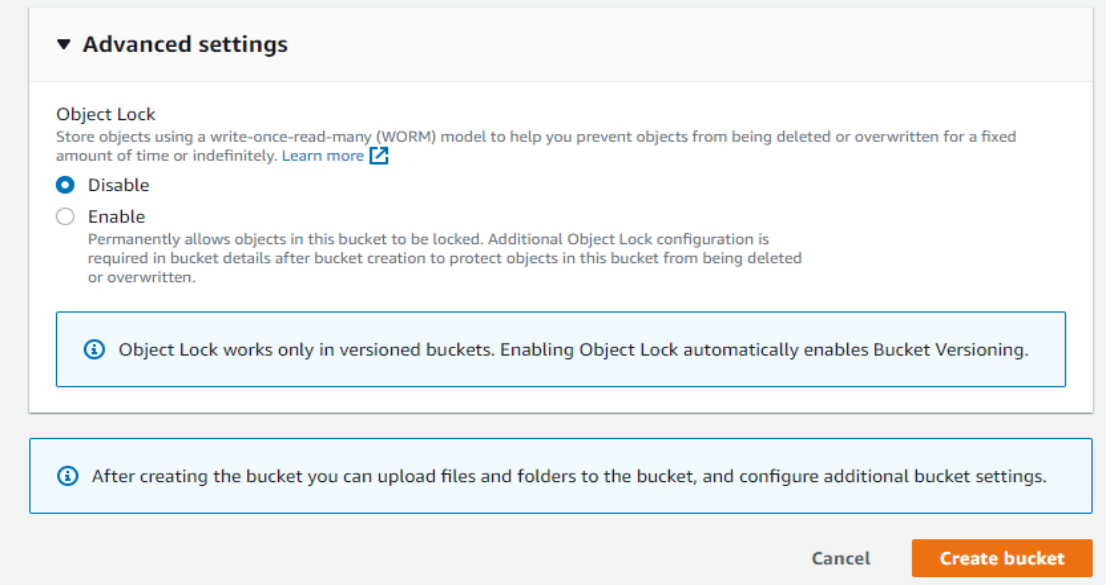


Figur 2.24. Objekteierskap i S3-konsoll

Deretter angir du eierskapet til objektene som lagres i samlingen. Vi velger den anbefalte innstillingen slik at tilgangskontrollisten (ACL) er deaktivert. Dette betyr at eierskapet til de lagrede objektene vil tilfalle til eieren av kontoen som beholderen tilhører.

Den andre innstillingen i dette bildet er Public Access. Med denne innstillingen kan du bestemme om objektene i samlingen skal være tilgjengelige fra andre kontoer, basert på de ulike kriteriene som er beskrevet i veiviseren.

Under de avanserte innstillingene kan vi stille inn beholderen til å ha en objektlås (se figuren ovenfor). Aktivering av objektlås betyr at objektene som lagres, ikke kan slettes eller endres mens låsen er i kraft. Dette kalles en Write-Once-Read-Many modell, eller WORM-modell.

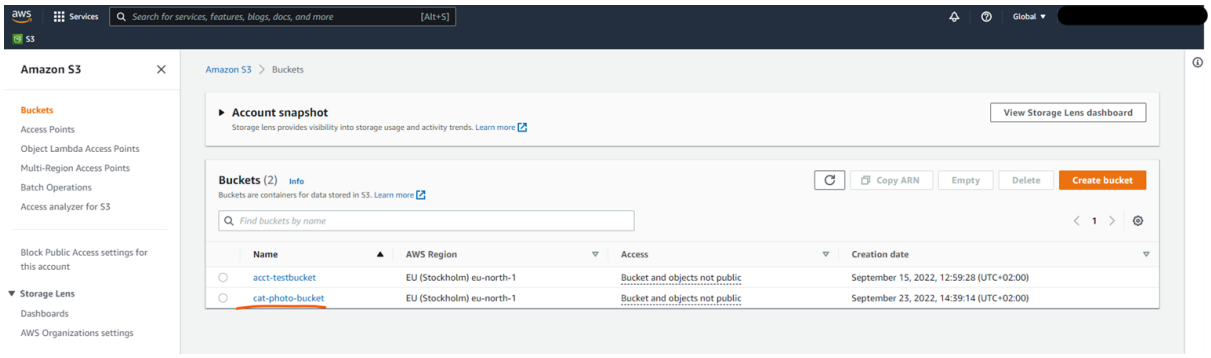


Figur 2.25. Etterbehandling konfigurasjon i S3-konsollen

Når all konfigurasjonen er gjort, klikker du på "Create bucket" -knappen.

Når du har opprettet beholderen, vil du bli tatt tilbake til S3-konsollen siden og den nye beholderenvil bli oppført i tabellen over beholdere og er nå klar til å lagre filene dine.

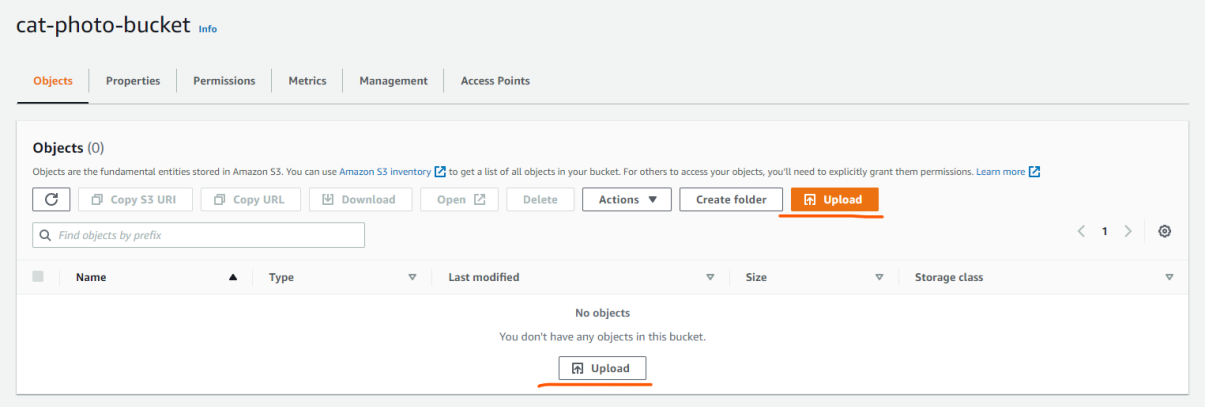
For å begynne å laste opp filer til denne nyopprettede beholdern, klikker du på navnet. Dette vil åpne beholderen (se figuren nedenfor).



Figur 2.26. Laste opp filer til nyopprettede beholdere i S3-konsollen - første trinn

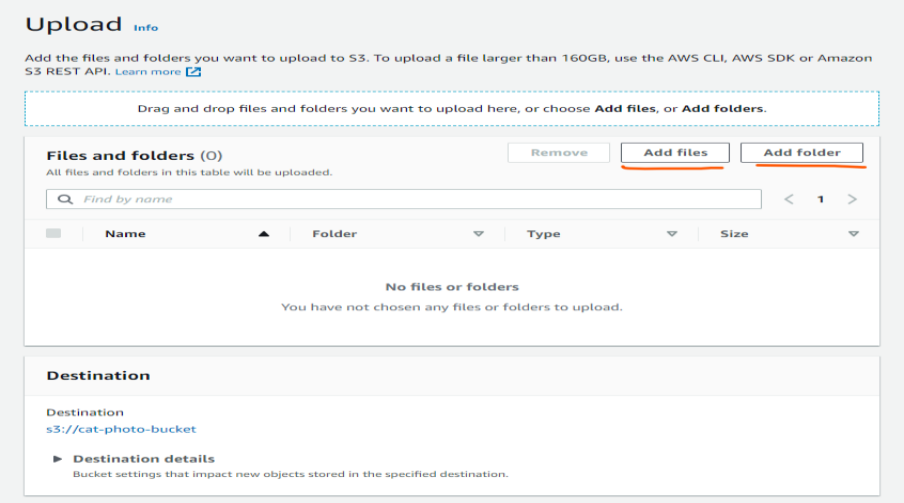
Her kan du se mye informasjon om samlingen, for eksempel objektene som er lagret i samlingen, og i egenskapsfanen kan du se og redigere noe av konfigurasjonen av samlingen som ble angitt under opprettelsen.

For å laste opp en fil til beholdere kan du klikke på en av de to Last opp-knappene, eller du kan dra og slippe filene fra filutforskeren din (se figuren nedenfor).



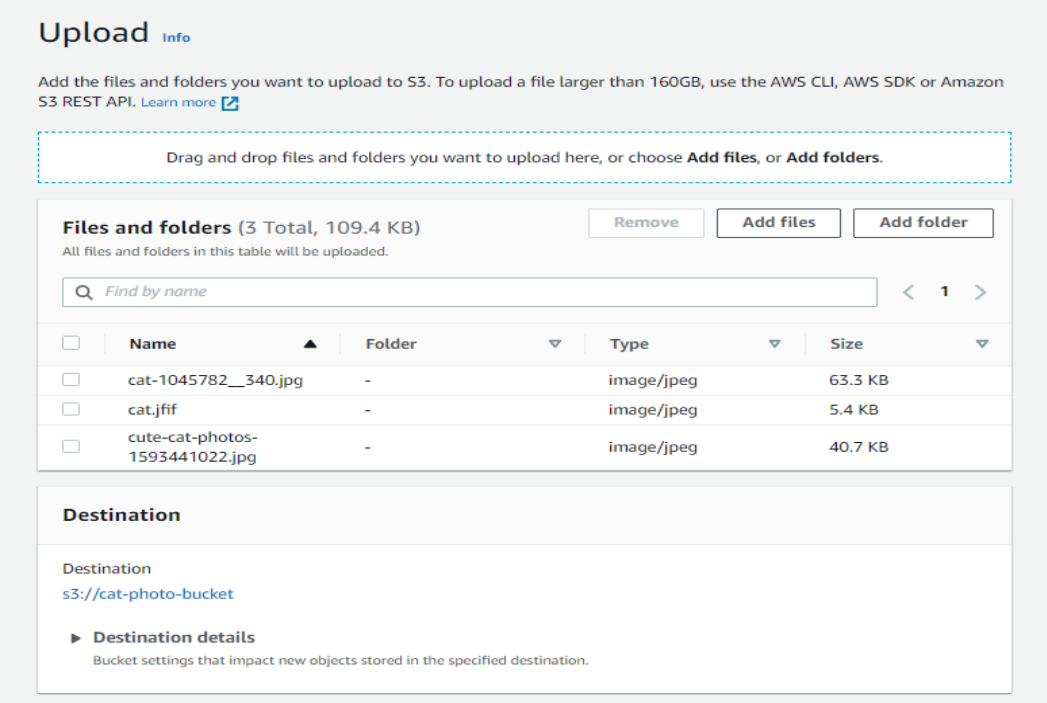
Figur 2.27. Laste opp filer til den nyopprettede beholderen i S3-konsollen - andre trinn

Ved å klikke på en av 'Last opp' -knappene tar du deg til neste skjermbilde, her får du valget mellom å laste opp individuelle filer, eller en hel mappe. Du kan enten klikke på "Legg til" -knappene, dette åpner en ny filutforsker, og du kan velge filene eller mappene du vil laste opp, avhengig av hvilken av de to knappene du klikket på.



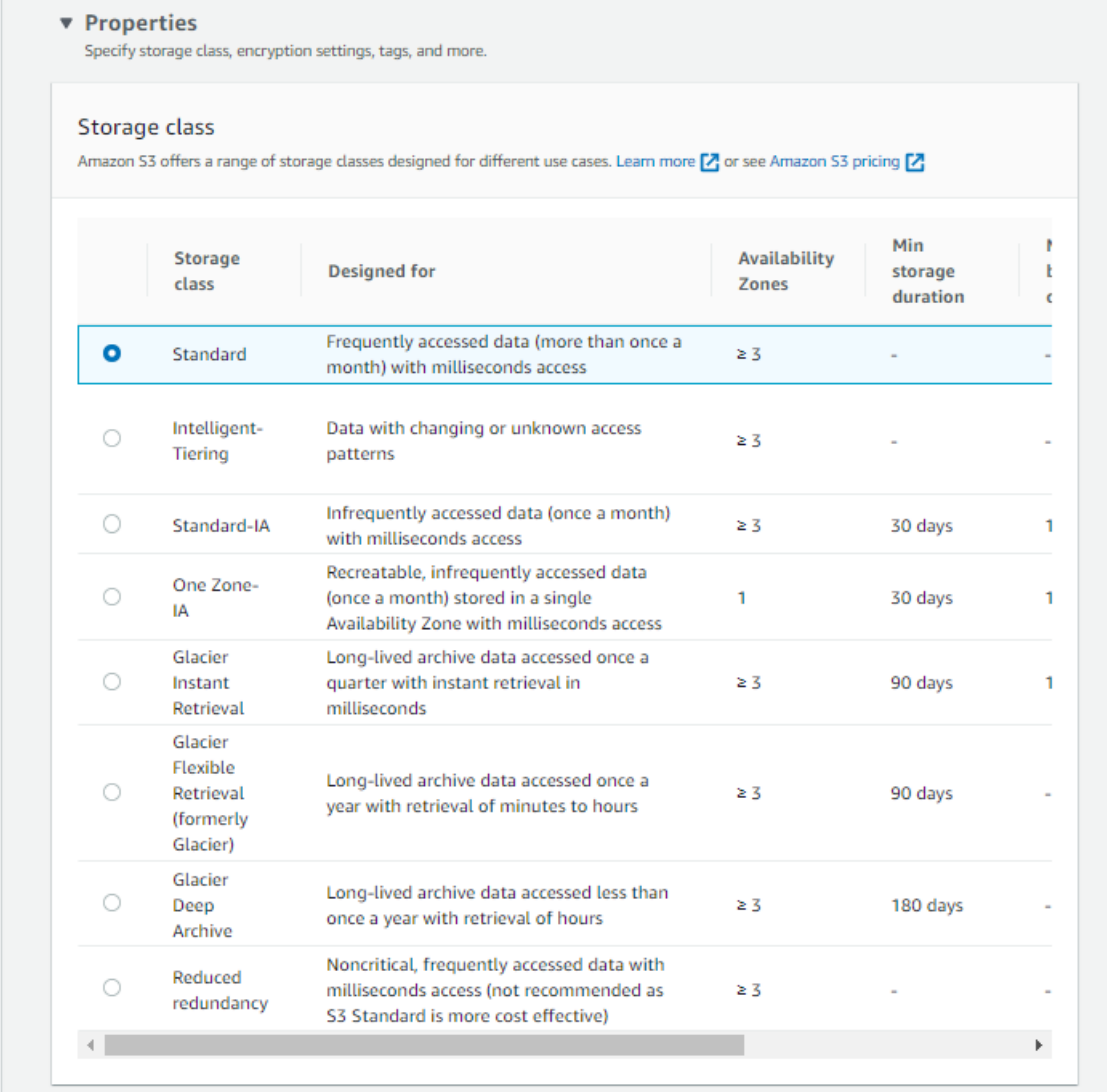
Figur 2.28. Laste opp filer til nyopprettet b i S3-konsollen - tredje trinn

I vårt eksempel har vi lastet opp tre bilder. Merk at destinasjonen er beholderen vi opprettet (se figuren nedenfor). Hvis du åpner destinasjonsdetaljene, vises noen avbeholderinnstillingene som ble angitt. Versjonskontroll, standardkryptering og objektlåsing.



Figur 2.29. Laste opp bilder til nyopprettet beholder i S3-konsollen

Så har vi egenskapene (se figur nedenfor). Det er her du kan angi hvilken lagringsklasse du vil bruke for filene eller mappene som lastes opp.

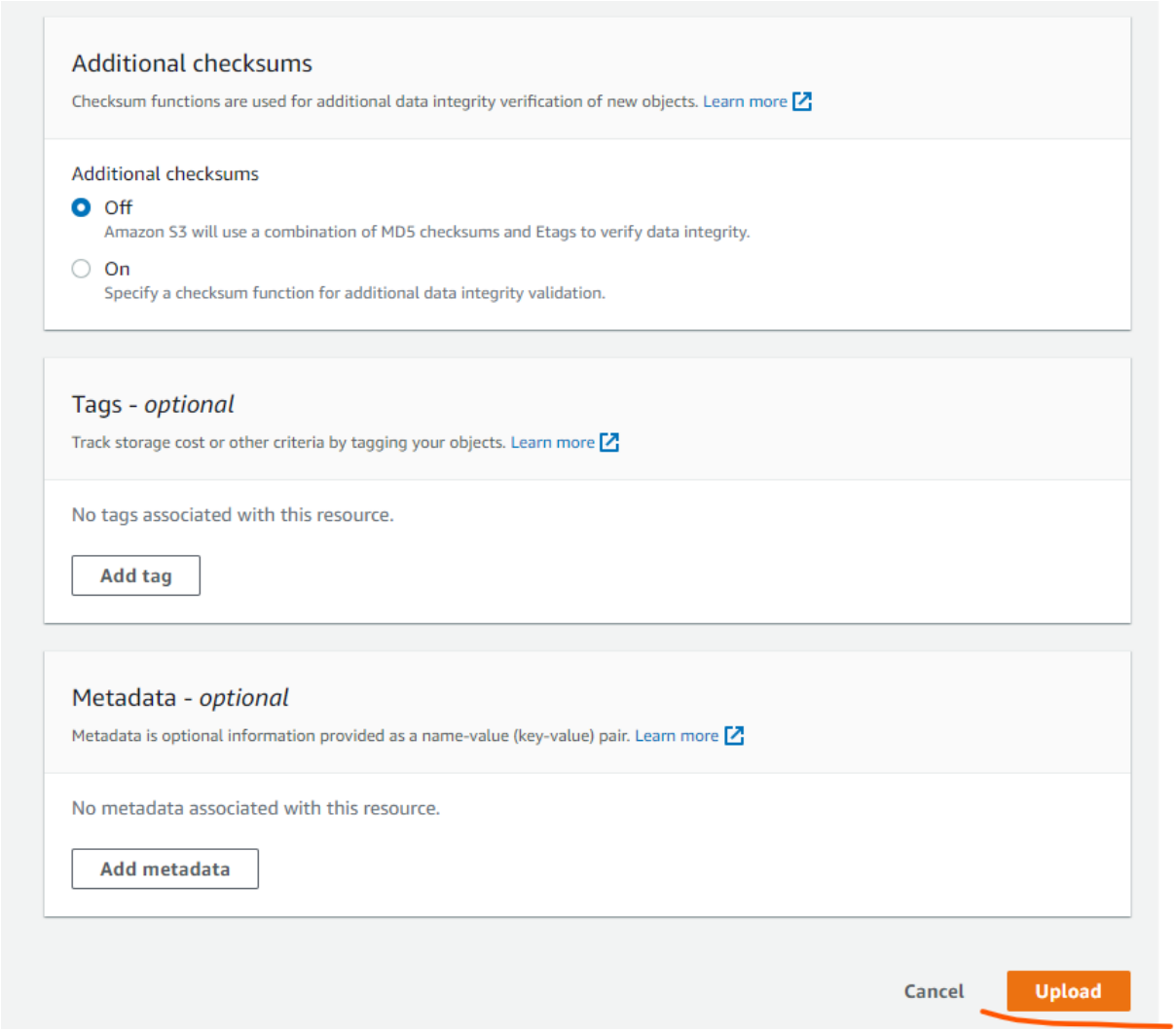


Figur 2.30. Egenskaper i S3-konsollen

Du kan også slå på flere kontrollsummer, slik at du kan sette din egen kontrollsumfunksjon for å sikre at integriteten til objektene er gyldig.

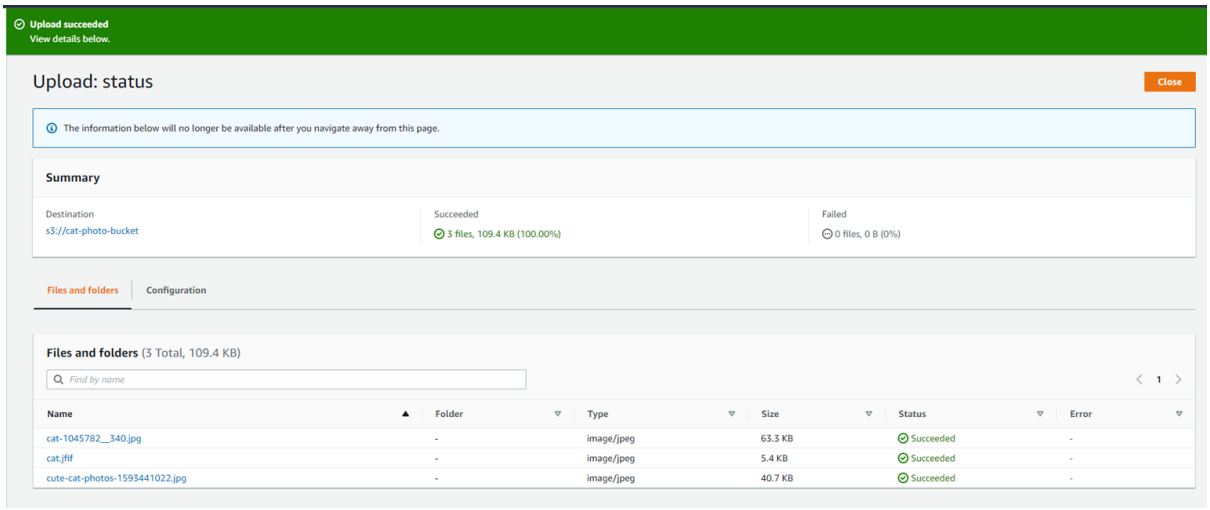
Koder ligner på de som ble nevnt tidligere under opprettelsen av samlingen, og metadata er data som på en eller annen måte beskriver selve dataene, for eksempel innholdstypen eller brukernavnet til personen som oppretter den opprinnelige filen.

Når alle disse er satt, klikker du på Last opp-knappen, og filene dine blir lagret i skyen (se figuren nedenfor)!



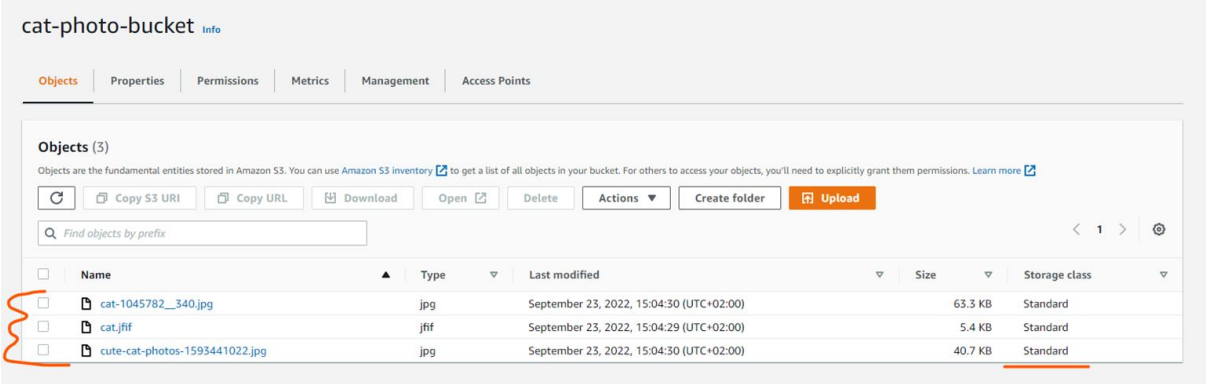
Figur 2.31. Last opp i S3-konsollen

Etter at opplastingen er fullført, ser vi at vi har en suksessmelding øverst, og vi kan se listen over våre tre bilder i fil- og mappetabellen med noen tilleggsdata om typen og størrelsen på filene og statusmeldingen.



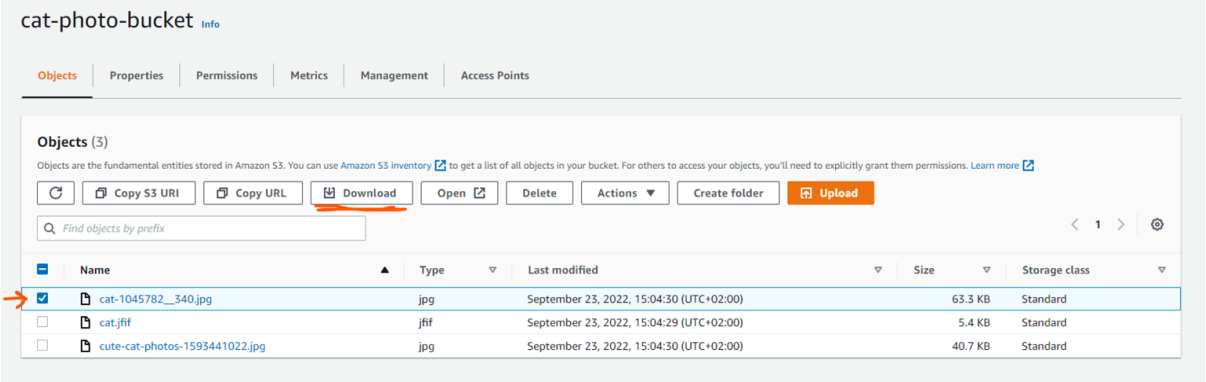
Figur 2.32. Vellykket-melding om opplasting i S3-konsollen

Ved å klikke på lukkeknappen blir vi tatt tilbake til beholderen vår, og vi kan nå se at vi har tre filer i objekttabellen vår, og litt informasjon om filene, for eksempel type, størrelse og hvilken lagringsklasse som brukes til å lagre den (se figur nedenfor).



Figur 2.33. Informasjon om de lagrede dataene i S3-konsollen

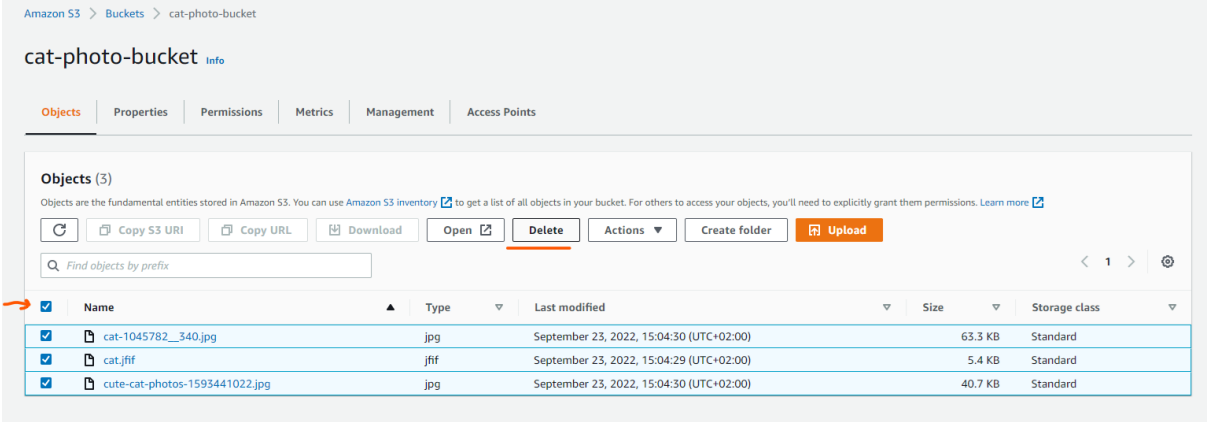
Nå som vi har filene våre i skyen, kan vi hente disse filene fra skyen. Merk av i boksen ved siden av navnet på filen du vil hente, og du vil legge merke til at de tidligere nedtonede knappene på raden over tabellen nå er tilgjengelige. Klikk på Last ned-knappen, så starter du nedlastingen av filen til datamaskinen din. Den kopierbare URL-en og S3 URI kan også brukes til å få tilgang til objektene, men i vårt tilfelle vil liming av URL-en i nettleseren bare gi deg en feilmelding om at vi ikke har tilgang.



Figur 2.34 Henter filer i skyen i S3-konsollen

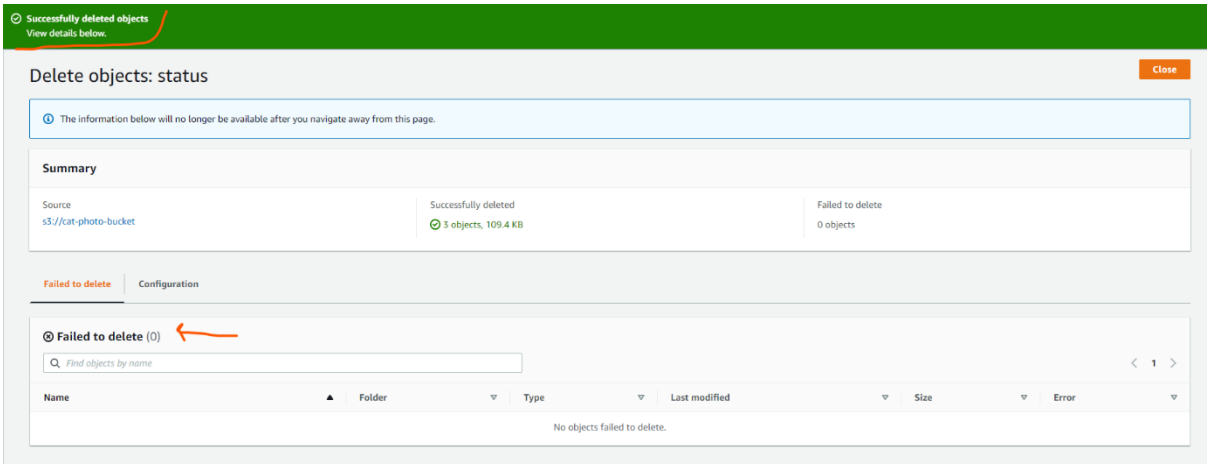
Noen ganger må du slette objekter fra en beholder (se figuren nedenfor). For å gjøre det må du bare velge filene eller mappene du vil slette, merke av i boksen ved siden hvor det står "Name", velge alle objekter i beholderen, eller velge hver enkelt fil som vi gjorde da vi hentet filen.

Etter at alle objektene du ønsker å slette er valgt, klikker du på sletteknappen.



Figur 2.35. Slette objekter fra en beholder i S3-konsollen

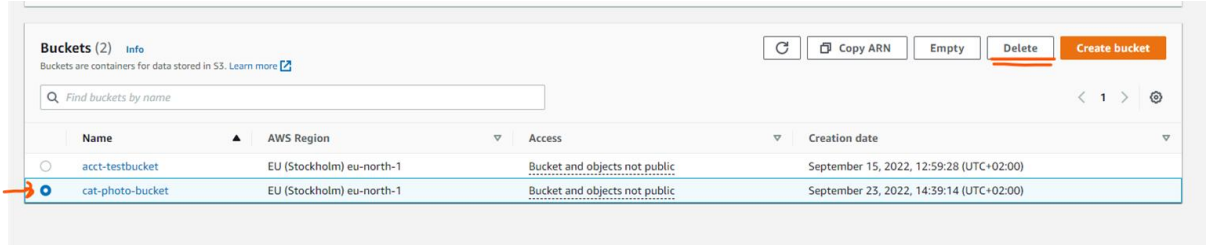
Etter å ha klikket på sletteknappen, blir du bedt om å bekrefte slettingen med en advarsel om konsekvensene av handlingen. Bekreft slettingen ved å skrive inn den ledede teksten 'slett permanent' i tekstfeltet og klikk på knappen for å fortsette. Etter at knappen er klikket, blir du omdirigert til et sammendrag av handlingen som viser om den var vellykket eller om det oppstod feil.



Figur 2.36. Slettet status i beholderen i S3-konsollen

Klikk lukk og du vil bli returnert tilbake til beholder-siden der alle objektene i beholderen nå har forsvunnet.

Nå som beholderen er tom, kan vi trygt fjerne den fra kontoen. For å slette selve beholderen, må du velge beholderen du vil slette ved å huke av knappen for riktig beholder og klikke på sletteknappen ved siden av Create bucket-knappen vi brukte tidligere (se figur nedenfor).



Figur 2.37. Slette bøtta i S3-konsollen

Som når vi slettet objektene i beholderen, blir du bedt om å bekrefte slettingen ved å skrive inn navnet på beholderen og klikke på Delete-knappen. Etter at slettingen er fullført, blir du omdirigert til hovedsiden S3, der beholderen din ikke lenger vil bli oppført i listen over beholdere.

2.3.3 Administrasjon av identitetstilgang

Identity Access Management (IAM) er en måte å håndtere både godkjenning av en aktør, det være seg en menneskelig bruker eller en maskin som får tilgang via en API, og autorisasjonen av den samme aktøren, og gir tilgang til medlemmene av en konto eller organisasjon til skyinfrastrukturen basert på tillatelsene de er gitt fra IAM-tjenesten.

IAM-tjenesten kan angi policyer på flere nivåer, for eksempel individuelle brukere eller for grupper.

Så hva er autentisering og autorisasjon, og hva er forskjellen?

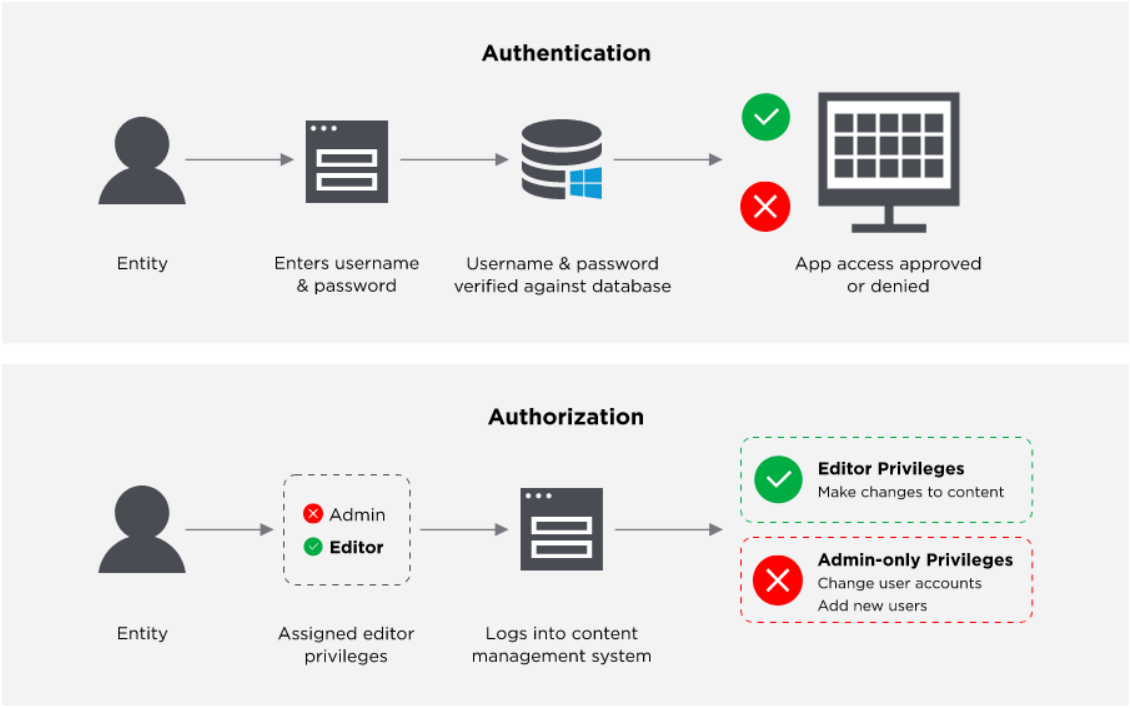
Autentisering er handlingen med å validere den som prøver å få tilgang til skyressursene dine, er den de hevder å være. Dette kan gjøres ved å bruke:

- Brukernavn og passord
  - Den vanligste måten å autentisere brukere på. Dette krever at den som prøver å logge inn oppgir en kombinasjon av brukernavn og passord som deretter sjekkes av et system, og hvis det samsvarer med det som er registrert i det systemet, har brukeren bekreftet at de er den de utgir seg for å være.
- EngangsPINs
  - Dette er en måte å validere på der brukeren ber om tilgang til systemet gjennom en automatisk generert PIN-kode som vanligvis bare varer i løpet av brukerens økt eller for en enkelt transaksjon.
- Autentiseringsapper
  - Et klarert tredjepartssystem genererer et passord som en bruker kan bruke.
- Biometri
  - Biometri krever at brukeren bekrefter sin identitet gjennom et fingeravtrykk, øyeskanning eller ansiktsgjenkjenning

Mer og mer ser vi Multi-Factor Authentication (MFA) blir brukt. Dette krever at den som prøver å autentisere seg selv gjennom to eller flere av de nevnte metodene. Disse metodene er ofte plassert i tre hovedkategorier; Noe du vet, noe du har og noe du er.

Disse vil veldig ofte være henholdsvis passordet ditt, en telefonapplikasjon og en biometrisk del som for eksempel ansiktsgjenkjenning.
Etter at brukeren har blitt verifisert, må de også godkjennes før de kan begynne å få tilgang til ressursene i skysystemet.

Autorisasjon er i denne sammenhengen en prosess der systemet kontrollerer om brukeren, som fra før er blitt autentisert, har tillatelsene som kreves for å utføre handlingen de prøver å utføre. Et eksempel på dette kan være et bildelager der vanlige brukere har lov til å se og laste ned bildene på nettstedet, men bare brukere med administratorrettigheter har lov til å laste opp bilder til depotet (se figur nedenfor).



Figur 2.38. Autorisasjon

Alle de tre store skytjenesteleverandørene tilbyr en identitets- og tilgangsadministrasjonstjeneste. Microsoft Azure kaller det Azure Active Directory. Amazon har kalt deres AWS IAM og i Google Cloud heter det bare IAM.

Identitets- og tilgangsadministrasjon hjelper deg med å kontrollere tilgangen til skytjenestene du bruker, for eksempel en AWS S3-beholder, eller en Microsoft Azure CosmoDB-instans. La deg opprette flere IAM-brukere under paraplyen til hovedkontoen din som håndterer alle ressursene.

Uten å bruke for eksempel AWS IAM for å administrere tilgangen til skyressursene dine, ville du ha måttet opprette flere AWS-kontoer, som hver ville ha en egen separate fakturering og abonnementer på de forskjellige AWS-produktene. Eller alle ansatte i organisasjonen din som trenger å bruke AWS, må dele legitimasjonen for en enkelt AWS-konto uten mulighet til å begrense de ansatte fra å få tilgang til ressurser de ikke trenger tilgang til.

Med IAM er det imidlertid mulig å sette opp flere brukere innenfor en enkelt AWS-konto, og starter med rotnivåbrukeren som AWS automatisk oppretter når du oppretter kontoen. Hver etterfølgende bruker som legges til kontoen, vil ha sin egen legitimasjon. Disse brukerne, enten de er mennesker eller maskiner, kan også få tilgang til spesifikke ressurser innen AWS gjennom bruk av retningslinjer som i AWS er definert i JSON-format (se figur nedenfor).

```
{
'Version': '2012-10-17',
'Statement': [{
    'Effect': 'Allow',
    'Action': 'iam:ListUsers',
    'Resource': '*'}]
}
```

Figur 2.39. Gi tilgang til spesifikke ressurser i AWS

Disse policyene er knyttet til brukere enten direkte eller via en brukergruppe.

En brukergruppe er en IAM-ressurs som du kan bruke til å legge til flere IAM-brukere i, slik at du enkelt kan knytte flere policyer til en hvilken som helst bruker ved å legge til brukeren i en brukergruppe. Hvis du for eksempel har en rolle i organisasjonen som krever at brukerne kan opprette og slette S3-beholdere, kan IAM-administratoren ganske enkelt legge til brukerens IAM-brukerkonto i brukergruppen når en ny person får denne rollen, i stedet for å knytte alle nødvendige policyer til brukeren manuelt.

Alle tre har den samme grunnleggende funksjonaliteten for godkjenning av brukerne som er knyttet til kontoen eller organisasjonen deres, og autoriserer disse brukerne til å få tilgang til ressursene de trenger tilgang til, gjennom policyer som er knyttet til brukerne på en eller annen måte.

IAM-ressurser

Bruker-, gruppe-, rolle-, policy- og identitetsleverandørobjektene som er lagret i IAM. Som med andre AWS-tjenester kan du legge til, redigere og fjerne ressurser fra IAM.

IAM-identiteter

IAM-ressursobjektene som brukes til å identifisere og gruppere. Du kan knytte en policy til en IAM-identitet. Disse inkluderer brukere, grupper og roller.

IAM-enheter

IAM-ressursobjektene som AWS bruker til godkjenning. Disse inkluderer IAM-brukere og-roller.

Aktører

En person eller et program som bruker AWS-kontoens rotbruker, en IAM-bruker eller en IAM-rolle for å logge på og sende forespørsler til AWS. Oppdragsgivere inkluderer fødererte brukere og antatte roller.

Modeller og prinsipper

Prinsippet om minste privilegium:

Prinsippet om minste privilegium, eller Just-Enough-Access, er en av hjørnesteinene i tilgangsstyring og sier at en bruker eller applikasjon bare skal tildeles akkurat nok tilgang som er nødvendig for å utføre oppgaven den gjør. Hvis et program for eksempel brukes til å vise bilder som lagres i et objektlager, for eksempel Azure Blob Storage, trenger det programmet bare å lese fra det lagringsområdet, som sådan bør det ikke gis noe utover lesetilgang.

Nulltillitsmodell:

Zero-trust-modellen er en sikkerhetsmodell der det antas at integriteten til nettverket har blitt kompromittert, og at det ikke er noen iboende sikre tilgangspunkter.

Dette er i strid med de eldre tradisjonelle sikkerhetsmodellene der et nettverk ble stengt fra resten av internett, og bare pålitelige og administrerte datamaskiner ville få lov til å bli med. Nettverket vil da gi tilgang til disse datamaskinene og enhetene basert på deres plassering og at de har fått tilgang til nettverket.

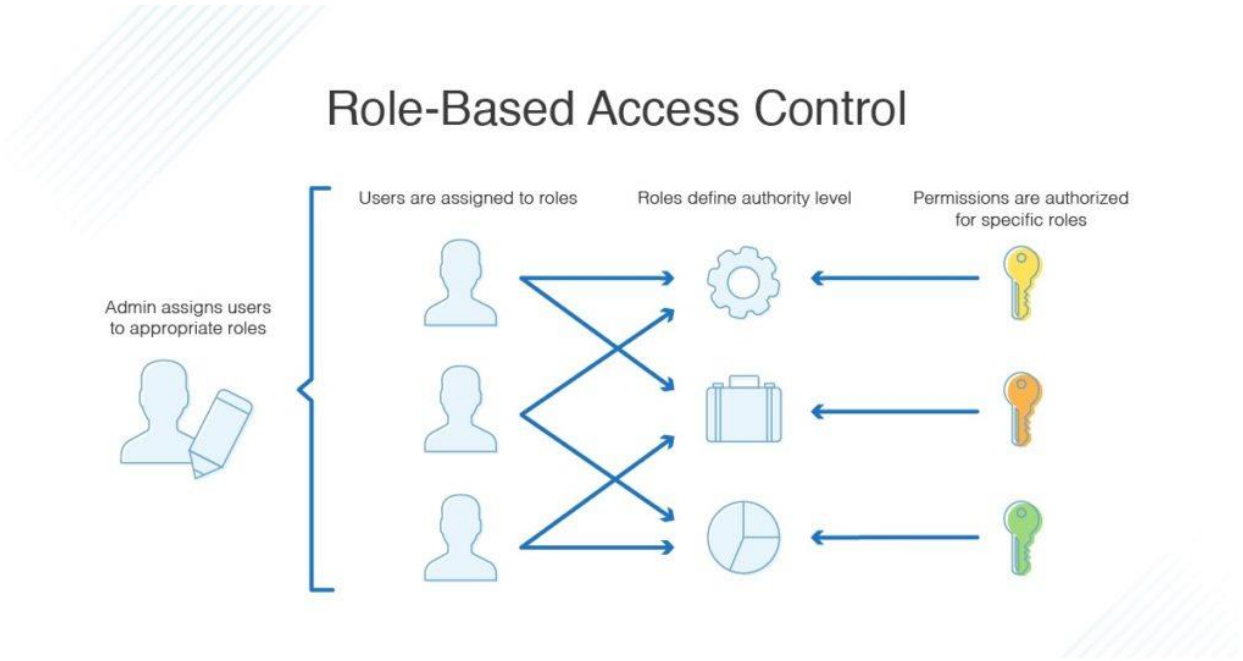
Med Zero-trust-modellen behandles alle enheter som om de kommer fra et usikkert sted, og krever at alle autentiserer for å bevise identiteten sin før de får tilgang til eiendelene og ressursene de trenger.

Just-in-time:

Just-in-time tilgang er en sikkerhetsmodell der en brannmur vil begrense all innkommende trafikk til en ressurs fram til en bruker ber om tilgang. Brukeren vil da få autorisasjonen sin kontrollert, og hvis forespørselen godkjennes, endres reglene for innkommende trafikk for den forespurte ressursen midlertidig for å tillate denne brukeren tilgang og deretter endre dem tilbake til å nekte trafikk.

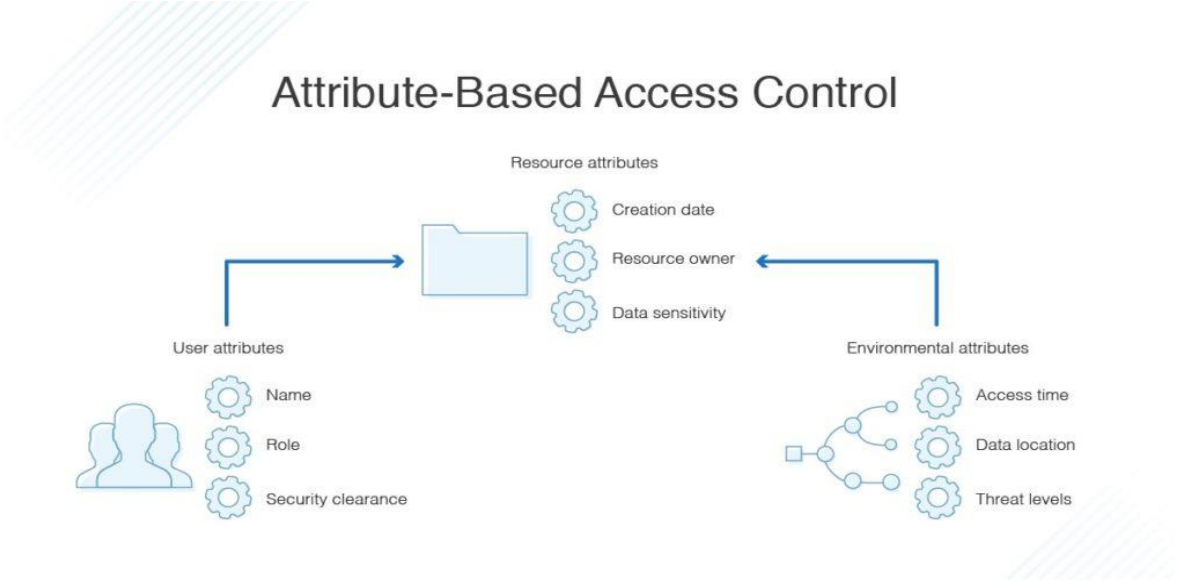
RBAC og ABAC

Rollebasert tilgangskontroll (RBAC) og attributtbasert tilgangskontroll (ABAC) er to av de vanligste metodene for å sikre tilgang til ressursene i skyen.



Figur 2.40. Rollebasert tilgangskontroll

I rollebasert tilgangskontroll gis tilgangen basert på rollene som er gitt til brukeren av administratoren av skyøkosystemet. Reglene for tilgang er definert i policyer som er tilordnet rollene. Eksempelroller kan være én rolle for en utvikler som trenger lese- og skrivetilgang til en database, og én rolle for en regnskapsfører som trenger tilgang til faktureringsinformasjonen for den samme databasen. Når en person trenger tilgang til ressursene i rollene, kan brukeren få denne rollen tilordnet. Én bruker kan også ha flere roller tilordnet, og én rolle kan ha flere brukere tilknyttet seg (se figuren 2.40.).



Figur 2.41 Attributtbasert tilgangskontroll

I et attributtbasert tilgangskontrollsystem gis tilgangen til ressurser til brukere basert på noen attributter som er definert i ressursens policy. Dette lar brukerne opprette nye ressurser som autoriserte brukere har umiddelbar tilgang til fordi de har fått tilgang via et attributt, for eksempel en tag. Dette betyr at administratoren ikke trenger å opprette eller oppdatere policyer for å gi tilgang til nye ressurser som opprettes (se figur 2.41.).

RBAC vs. ABAC- fordeler og ulemper

ABAC-fordeler

- Høy grad av kontroll og granularitet
- Kan unngå tidkrevende arbeid når du administrerer en overveldende mengde roller
- ABAC ulemper
- Kan være tidkrevende å sette opp
- Må gjennomføres helt fra begynnelsen
- RBAC-fordeler
- Enkle å bruke og enkle, mindre komplekse regler
- RBAC-ulemper
- Kan føre til rolleeksplosjon der man må håndtere et for stort antall forskjellige roller
- Når skal jeg velge en RBAC-modell?
- Små bedrifter som administrerer få skyressurser og med små team hvor det er liten risiko for "rolleeksplosjon"
- Hvis organisasjonsstrukturen er enkel og med veldefinerte roller.

Når skal jeg velge en ABAC-modell?

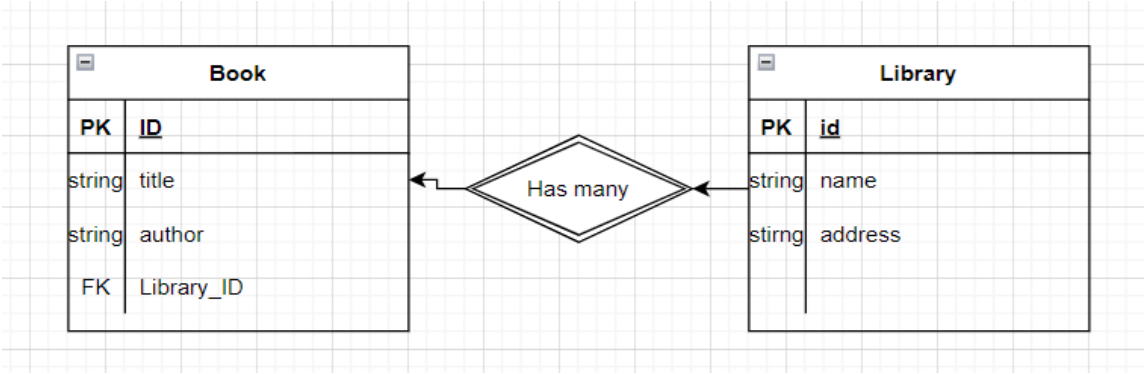
- Hvis du jobber med midlertidige eller distribuerte team der du kanskje må gi tilgang basert på stedet de har tilgang fra og tidssonene de er i.
- Hvis det er mye samarbeid om filer og dokumenter der tilgangen må baseres på typen dokument/fil i stedet for rollen som vil ha tilgang til den.
- I mange tilfeller vil du ha en kombinasjon av begge modellene der RBAC gir tilgang på et høyere nivå, men bruk ABAC for å oppnå en finere, mer detaljert kontroll.

2.3.4 Databasetjenester i skyen

Når du velger en database og database leverandør er det, som med å velge lagringstype / leverandør, mange forskjellige hensyn som må tas. Det finnes flere forskjellige typer databaser, og de har alle sine styrker og svakheter, avhengig av hva slags data som lagres.

De tradisjonelle relasjonsdatabasene som bruker SQL (Structured Query Language), for eksempel mySQL eller PostgreSQL, er flotte når du arbeider med datasett som er veldefinerte fra starten, og der det ikke vil være noen endringer i formatet på dataene over tid, og det er sterke og klare relasjoner mellom de ulike delene av datasettet.

Du kan for eksempel ha relasjonen mellom en bok og et bibliotek. I dette tilfellet vil et bibliotek ha mange bøker, men en bok kan bare tilhøre et enkelt bibliotek (se figur 2.42.).



Figur 2.42. Forholdet mellom boken og biblioteket

Men noen ganger er dataene du har ikke godt strukturert, og du har mindre kontroll over hvordan dataene kommer til å endre seg over tid. For disse tilfellene kan det være best å bruke en NoSQL (Not only SQL) database ....

Amazon RDS (Relational Database Service) støtter en rekke av de mest populære relasjonsdatabasene som mySQL, MariaDB og OracleSQL, men tilbyr også sin egen relasjonsdatabase kalt Amazon Aurora.

Microsoft Azure tilbyr flere relasjonsdatabasetjenester, for eksempel Azure SQL Database og Azure Database for PostgreSQL/MariaDB/MySQL.

Google Cloud Platform har Cloud SQL, AlloyDB og Cloud Spanner. De har også en løsning som er optimalisert for datalagerhus kalt BigQuery.

For NoSQL-løsningene tilbyr Google sin egen dokumentdatabase kalt Firestore og en nøkkelverdidatabase kalt Cloud Bigtable.

Microsoft Azure har en NoSQL-løsning kalt Cosmos DB som støtter en rekke andre NoSQL API-er, for eksempel Apaches Cassandra og MongoDB, men har også støtte for SQL.

Amazons NoSQL-tjenester inkluderer DocumentDB og DynamoDB som begge administrerte tjenester.

Når du velger type database og leverandør, må det tas noen hensyn. Viktige ting å vurdere er hvilken type data som blir lagret. Er dataene svært strukturert med sterke relasjoner? Det beste valget kan være en relasjonsdatabase.

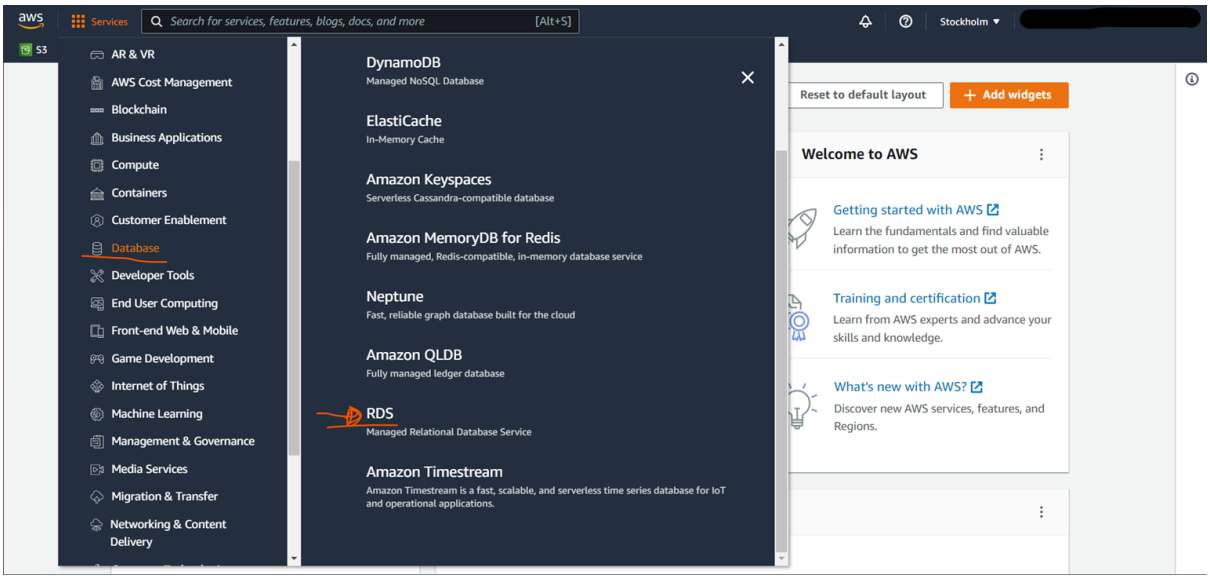
I tillegg til å bestemme hvilken type database som passer best, er det viktig å bestemme hvilken instansklasse som trengs. DB Instanse-klassene bestemmer mengden minne, CPU, og I/O-gjennomstrømningen som er tilgjengelig for databaseserveren.

DB-sikkerhet: Nærhet til internett. - Virtuell privat sky. Network gateway, tilgangskontroll bruker IAM, brukere og roller kan brukes til å bestemme tilgang til DB-handlinger (Getting, Posting)

AWS bruker AES-256 mens den er i ro.
Amazon tilgjengelighetssoner for å øke holdbarheten i tilfelle infrastrukturfeil.

En praktisk gjennomgang for hvordan du instansierer en database med Amazon RDS ved hjelp av Amazon Aurora MySQL (se figur 2.43.):

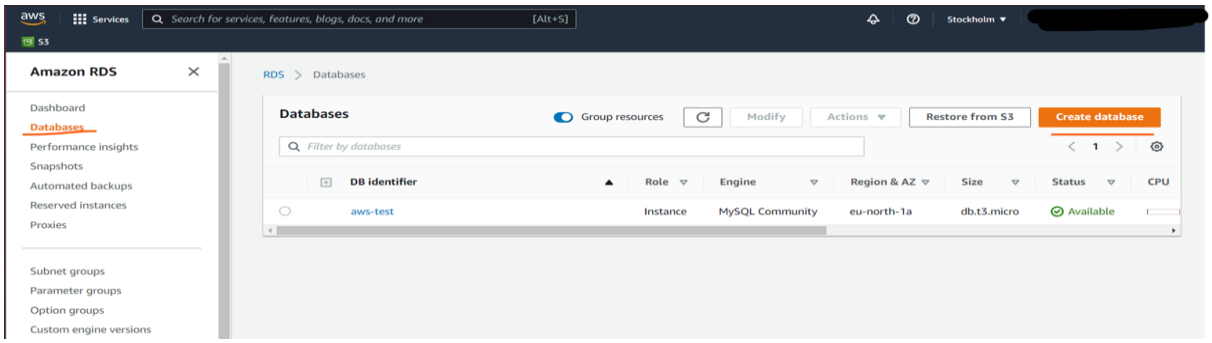
Når du er på AWS-konsollens hjemmeside, klikker du på Tjenester-knappen øverst til venstre og finner deretter 'Database' i rullegardinmenyen. Klikk på den og en ny rute åpnes. Finn 'RDS' og klikk på den.



Figur 2.43. Database med Amazon RDS ved hjelp av Amazon Aurora MySQL

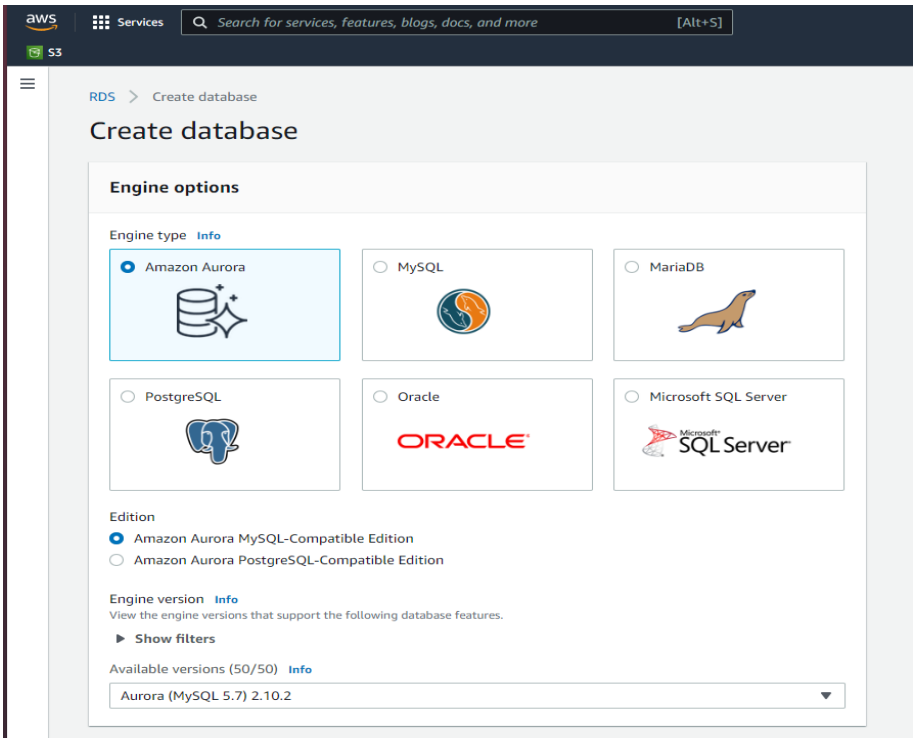
På Amazon RDS-konsollens hjemmeside, klikk på Databaser på menyen til venstre, dette tar deg til panelet med oversikt over alle databaser som er koblet til AWS-kontoen din.

For å opprette en ny database, klikker du på knappen som sier 'Create database' som åpner veiviseren for databaseoppretting (se figur 2.44.).



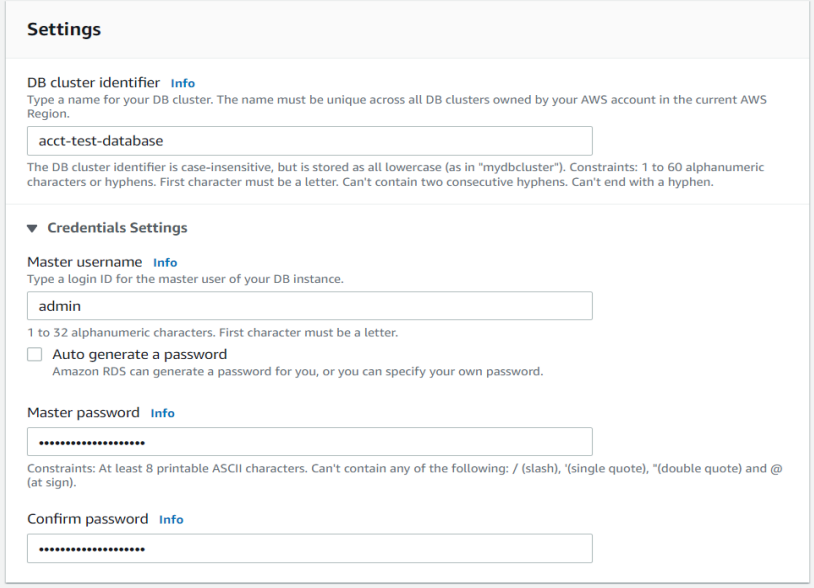
Figur 2.44. Opprettelse av en ny database – første trinn

I veiviseren får du flere alternativer for hvilken relasjonsdatabase du ønsker å bruke, og også hvilke versjoner av databasemotorene du vil bruke. Vi forlater standarden, velger Amazon Aurora MySQL-kompatibel utgave og får den til å kjøre på MySQL 5.7-versjonen (se figur 2.45.).



Figur 2.45. Opprettelse av en ny database – andre trinn

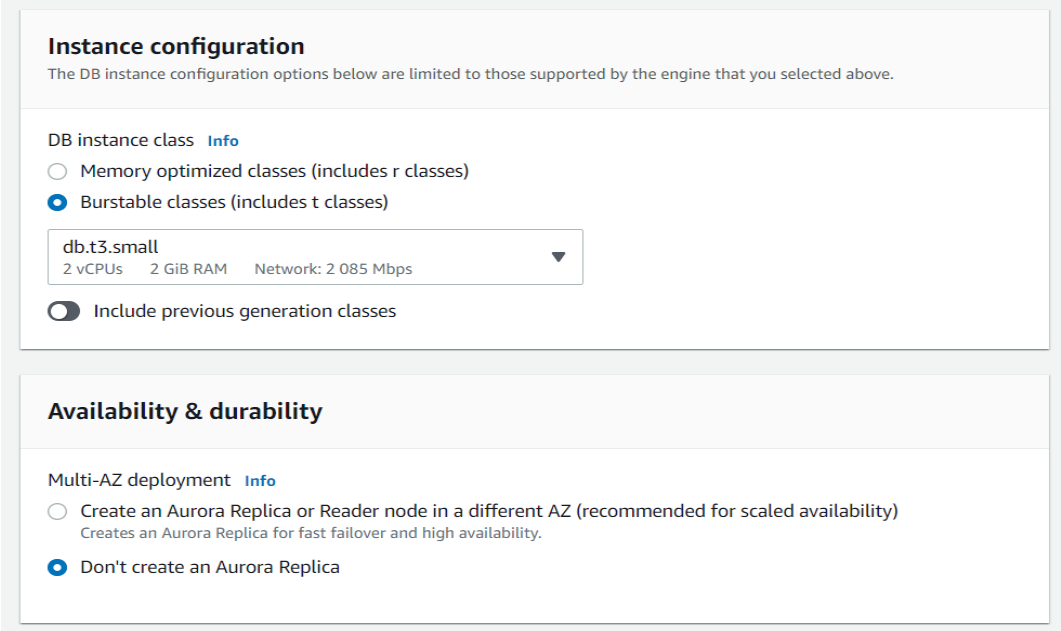
Ruller ned kan vi angi innstillingene for databasen, definere klyngenavnet (eller bare databasenavnet hvis du bruker mysql) og legitimasjonen som brukernavn og passord (se figur 2.46.).



Figur 2.46. Innstillinger for databasen

I konfigurasjonsinnstillingen for instansen bestemmer du hvilken instanseklasse som skal brukes for databasen. I vårt tilfelle vil vi velge den minste skalerbare klassen av kostnadshensyn, men i en reell applikasjon må man vurdere hva slags datasett den skal håndtere, og hva slags tilgangsmønstre og hva slags I/O-gjennomstrømning den trenger å håndtere.

Oppretting av en Aurora-replika kan velges for å opprette replikaer i forskjellige tilgjengelighetssoner, slik at hvis en AZ går ned eller opplever problemer, kan du raskt bytte til en annen AZ med minimal nedetid (se figur 2.47.).



Figur 2.47. Opprette en Aurora-kopi

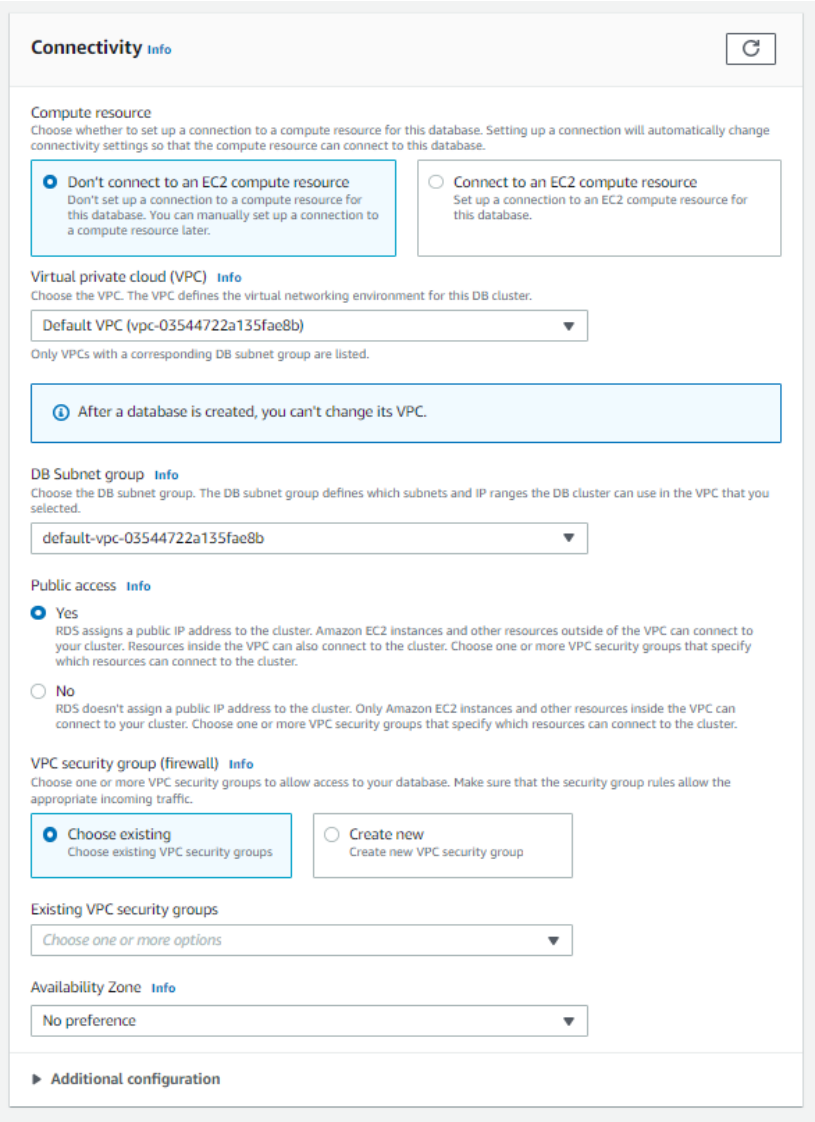
I tilkoblingsinnstillingene (se figur 2.48) vil du sette opp om du vil koble databasen din til en Amazon Elastic Cloud Compute eller EC2-ressurs.

Det er også nødvendig å opprette en Virtual Private Cloud (VPC). I denne VPC-en kan du opprette spesielle regler for hvem som har tilgang til ressursen i den.

Subnettgruppen brukes til å definere hvilke IP-adresser databasen har tillatelse til å bruke i VPC. Vi lar begge disse være standard.

Offentlig tilgang definerer om noe eller noen som ikke er innenfor VPC, kan få tilgang til databasen via en offentlig IP-adresse opprettet av veiviseren. Vanligvis vil du deaktivere dette, slik at bare ressurser som er inne i VPC-en, får tilgang til databasen, noe som minimerer risikoen for uautorisert tilgang.

VPC-sikkerhetsgrupper er som tilgangslister der IP-adresser har tilgang til databasen.

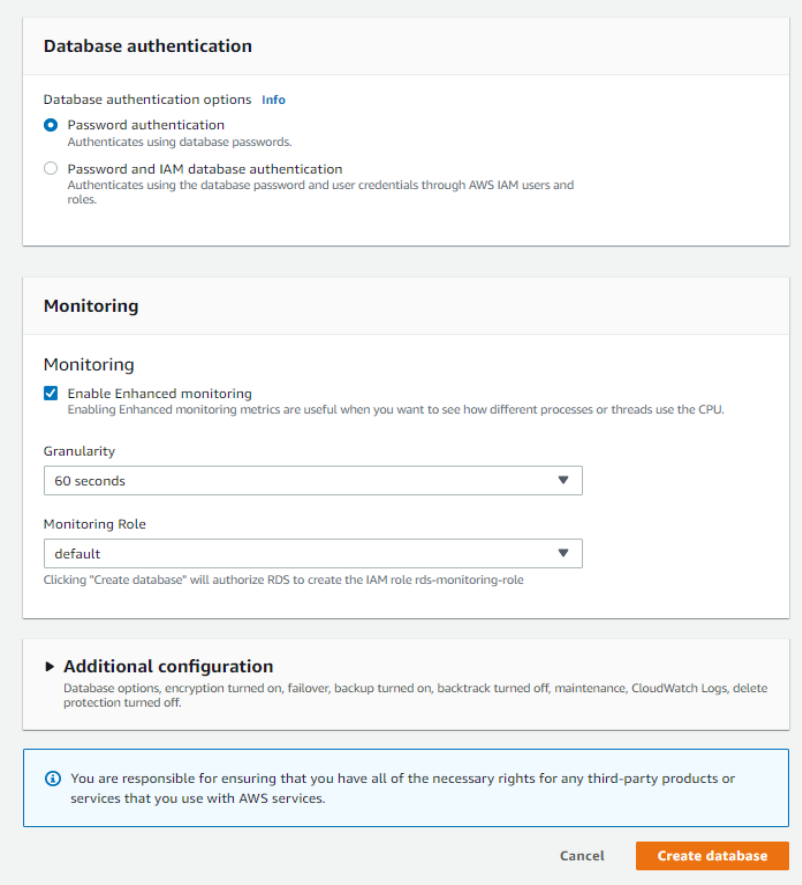


Figur 2.48. Innstillinger for tilkobling

Du kan velge hvilken tilgjengelighetssone i ditt område du foretrekker at databasen skal være plassert i.

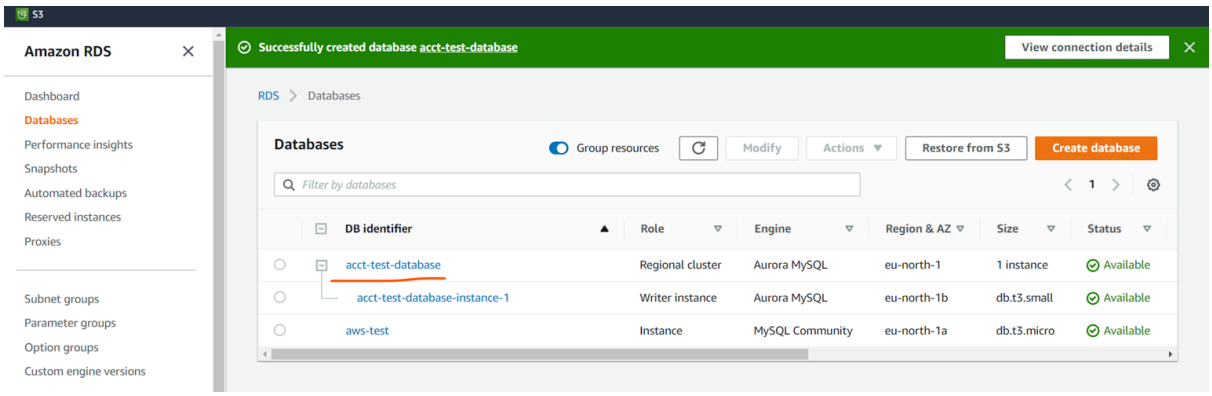
Autentiseringen lar deg bestemme om bare databasepassordet er nok, eller om noen autentisering også må inkludere en AWS IAM-bruker/rolle.

Overvåking overvåker ressursbruken til databasen. Nå som vi har konfigurert alle innstillingene våre, kan vi opprette databasen vår. Klikk på opprett database-knappen (se figur 2.49.).



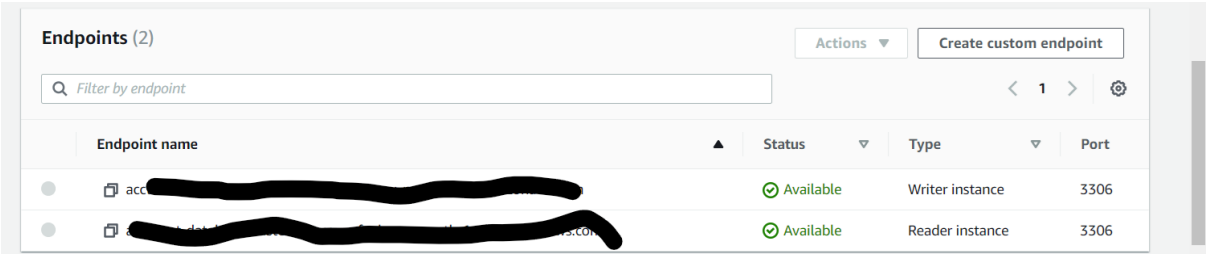
Figur 2.49. Opprette database

Databasen vår er opprettet, og vi kan nå se den i listen på Amazon RDS-konsollsiden vår (se figur 2.50).



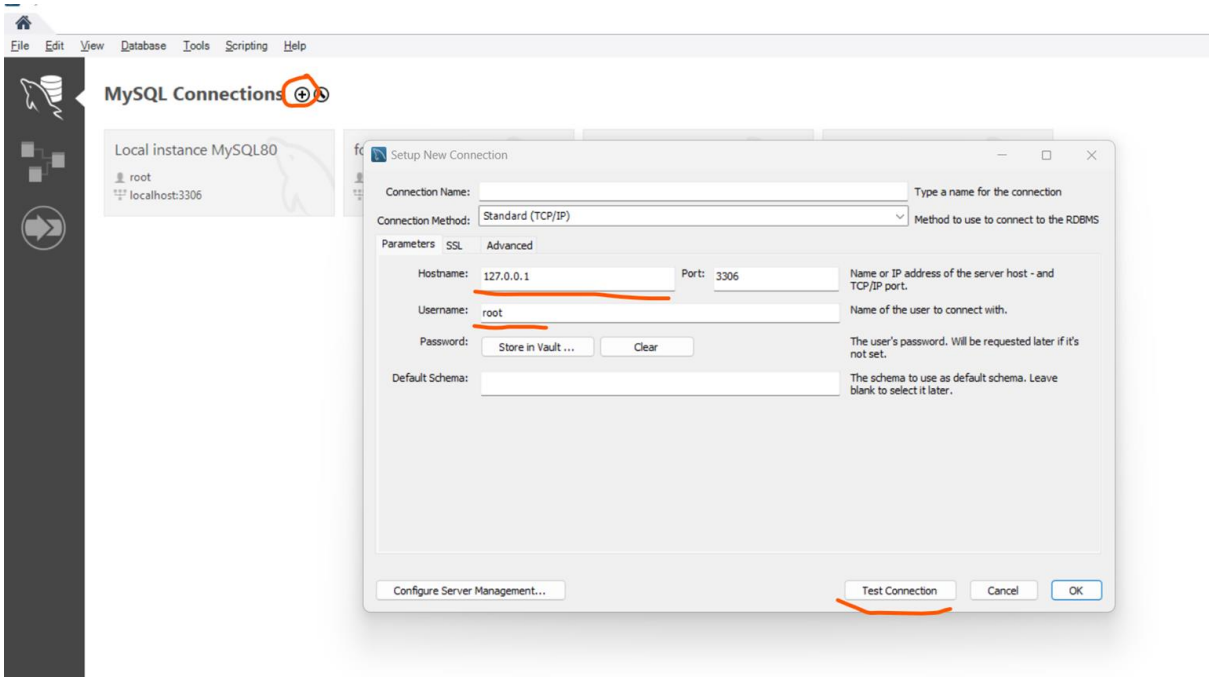
Figur 2.50. Opprettet database synlig i Amazon RDS-konsollsiden

Nå som vi har opprettet databasen vår, vil vi koble til den og lage noen tabeller. Ved å klikke på navnet på databasen vi nettopp opprettet, kan vi se endepunktet til databasen (se figur 2.51). Dette er adressen vi må koble til.



Figur 2.51. Endepunkter for opprettet database

Deretter skal vi bruke MySQL Workbench for å koble til denne databasen. Ved å klikke på den innsirklede plussen ved siden av der det står "MySQL-connections," åpnes vinduet i bildet. Vertsnavnet er hvor du vil lime inn endepunktet fra serveren, og brukernavnet vil være hoved-DB-brukernavnet du valgte da du opprettet databasen. Etter at du har skrevet inn disse to, kan du klikke på 'test connection'. Du vil da bli bedt om å oppgi passordet du angir, og hvis alt dette fungerer, vil du få en melding som sier at en tilkobling ble opprettet. Du kan deretter gi tilkoblingen et navn og klikke OK.



Figur 2.52. Bruke MySQL arbeidsbenk for tilkobling til ny database

Etter vellykket tilkobling til databasen og logget inn vil du kunne begynne å lage databaser med tabeller og informasjon ved hjelp av SQL-uttrykk.

2.3.5 Vurderinger for domenekonfigurasjon

I denne enheten vil du lære at når du velger riktig skytjenesteleverandør, bør bedrifter vurdere mer enn bare produktpakke. Nesten alle selskaper bruker en leverandør av infrastruktur som en tjeneste (IaaS) eller plattform som en tjeneste (PaaS). Organisasjoner vil sannsynligvis starte med en av tre skyleverandører, Amazon Web Services (AWS), Azure eller Google Cloud Platform (GCP), og kan bestemme seg for å redusere risikoen ved å tilby en mangfoldig tjenestebase gjennom flere leverandører, optimalisere ved å distribuere de riktige arbeidsbelastningene i riktig sky og minimere leverandørlåsing.

Viktige forskjeller mellom skyplattformer

1. En titt på Amazon Web Services (AWS)

Da AWS først ble lansert i 2006, leverte de først og fremst databehandlings-, lagrings- og databasetjenester som ble brukt av utviklere. Som den første skyleverandøren forblir AWS nyskapende fordi den hadde et tidligere fundament å bygge videre på.
De fleste selskaper bruker følgende tjenester på AWS:

- AWS Elastic Compute Cloud (EC2): skalerbar, skalerbar datakraft for programvarehosting eller maskinlæring
- AWS Relational Database Service (RDS): En tilpassbar databasemotor for hosting av databaseservere og arbeid med NoSQL-databaser.
- AWS Lambda Functions as a Service (FaaS): Hendelsesdrevet serverløs databehandling for bakgrunnsprosesser som bildetransformasjon, databehandling i sanntid og validering av streamingdata.
- AWS Simple Storage Service (S3): i første omgang for utviklere med vedvarende lagring, men også for arkivering og kostnadseffektiv datamigrering
- AWS Elastic Container Service (ECS): Containeradministrasjon for å starte, stoppe og administrere klyngecontainere.
- AWS CloudFront Content Delivery Network (CDN): Lagrer data på kanten for å levere data, video, bilder, applikasjoner og APIer.

2. Hva tilbyr Azure?

Azure har en tendens til å fremme bedriftsorganisasjoner som allerede har investert i Microsoft-produkter og -tjenester.

De fleste Azure-selskaper bruker følgende tjenester:

- Azure Hybrid: En tjeneste for arbeidsbelastninger som kombinerer lokale Windows Server- og SQL Server-lisenser

- Azure Virtual Desktop (AVD): Virtual Desktop Interface (VDI) for ekstern tilgang til Windows 10 og programmer
- Azure Sentinel: Security Information Event Management (SIEM) og Security Orchestration Automated Response (SOAR) for oppdagelse, synlighet og respons på trusler
- Azure Cosmos DB: NoSQL-database med åpent API for mobil-/nett-, spill- og e-handels-/detaljhandelsprogrammer
- Azure Active Directory (AD): En identitetstjeneste som synkroniserer Microsoft-miljøer lokalt og i skyen med enkel pålogging og godkjenning med flere faktorer.

3. Google Cloud Platform (GCP) og hvordan de sammenlignes

For ikke å bli overgått, lanserte Google en betaversjon av GCP i 2008. Mens AWS tilbyr IaaS-tjenester, fokuserte GCP i utgangspunktet på PaaS-tjenester. Utviklere kan utvikle og kjøre nettprogrammene sine i datasentre som administreres av Google. Over tid har GCP utvidet tilbudet sitt til å omfatte Google-pakker, stordatateknologier og administrasjonsverktøy.

GCP fokuserer generelt på utviklere som ønsker å bygge og kjøre programmer. Det har en tendens til å fokusere på organisasjoner som ønsker å bygge applikasjoner, men mangler lokale datasentre for å støtte dem.

De fleste bedrifter bruker følgende tjenester i GCP:

- Google Compute Engine: En forhåndskonfigurert eller tilpassbar kjernebasert virtuell maskin (KVM) for Linux- og Microsoft-servere
- Google Cloud Storage (GCS): blokk-, fil- og objektlagring med regler for livssyklusadministrasjon for forskjellige datatyper
- Google Kubernetes Engine (GKE): Et administrert, administrert stagingmiljø for distribusjon av mikrotjenester
- BigQuery Machine Learning (ML): Maskinlæringsmodeller for bedriftsinnsikt

Hvor mange tilgjengelighetsområder har hver leverandør?

Dette er viktig når man bestemmer et selskaps samsvarskrav, som i henhold til General Data Protection Regulation (GDPR), bør selskaper lagre og behandle data i et av EU-landene.

Slik er konkurrentens rangering:

- AWS: 26 geografiske regioner
- Azure: 60+ områder
- GCP: 29 regioner
- Hvert område har vanligvis flere tilgjengelighetssoner. Dette betyr at du bør vurdere følgende:
- AWS: 84 tilgjengelighetssoner totalt

- Azure: 3 tilgjengelighetssoner per område, minst 180 totalt
- GCP: 88 tilgjengelighetssoner
- Ytterligere hensyn kan omfatte spesialiserte tjenestealternativer som hver leverandør har som er forskjellige:
- AI/maskinlæring
- Tingenes Internett (IoT)
- Augmented reality / virtuell virkelighet
- Forretningsanalyse
- Robotteknologi.

Prisstruktur

Hver av de tre store leverandørene tilbyr forskjellige prismodeller basert på en organisasjons skybruk. Alle tre leverandørene synes priser og fakturering er vanskelig, noe som betyr at du må være oppmerksom på følgende når du vurderer hvilken server du skal bruke:

- Styresett
- Faktureringsformat
- Overvåk forbruk og budsjett
- Endringer i prismodellen
- Langsiktig kontra forbruksbasert prisverdi.

Styringsverktøy

Som allerede nevnt, kan du bruke forskjellige skytjenester for å kombinere ressurser og verktøy for å effektivisere og sentralisere forretningsbehov. Det er imidlertid viktig å merke seg at AWS og Azure er mer forretningsorienterte enn GCP, og AWS tilbyr det største utvalget innen outsourcede tjenester. Dette kan være en viktig faktor for de virksomhetene som trenger de mest robuste alternativene (se figur nedenfor).

Her er en figur (diagram) som beskriver forskjellene:

Management and governance

	AWS	Azure	Google Cloud
Automation	AWS CloudFormation, AWS Proton, AWS OpsWorks	Azure Resource Manager, Azure Automation	Cloud Deployment Manager, Cloud Foundation Toolkit, Cloud Scheduler
Anomaly detection	CloudWatch Anomaly Detection	Anomaly Detector	Anomaly Detection
Application portfolio and data governance	AWS Service Catalog	Azure Managed Applications, Azure Blueprints (preview), Azure Purview (preview)	Dataplex, Private Catalog, Service Directory
Automated Windows Server management	N/A	Azure Automanage (preview)	N/A
Configuration management	AWS Config	Azure App Configuration	Cloud Asset Inventory
Health dashboard	Personal Health Dashboard	Resource Health, Azure Service Health	Cloud Monitoring
Hybrid and multi-cloud management	Amazon EKS Anywhere (preview), Amazon ECS Anywhere	Azure Arc	Google Anthos, Network Connectivity Center (preview)
License management	AWS License Manager	N/A	N/A

Figur 2.53. Liste over ulike skytjenester

Også nøkkelen til administrasjonstjenester er de som bruker IoT-verktøy og hvordan de er forskjellige (se figur 2.54.).

IoT

	AWS	Azure	Google Cloud
Cloud-device connections, data collection and management	AWS IoT Analytics, AWS IoT Core, AWS IoT Device Defender, AWS IoT Device Management, AWS IoT Events, AWS IoT SiteWise	Azure IoT Central, Azure IoT Hub, Azure Defender for IoT, Azure Sphere	Cloud IoT Core
IoT edge compute	AWS Greengrass	Azure IoT Edge, Azure Percept (preview)	Edge TPU
Microcontroller OS	FreeRTOS	Azure RTOS	N/A
Virtual modeling	AWS IoT Things Graph	Azure Digital Twins	N/A

Figur 2.54. Forvaltningstjenester, som bruk IoT-verktøy

Spørsmål å vurdere:

- Hva er de viktigste forskjellene mellom de tre serverne, og hvilken plattform vil være mer attraktiv for en oppstart av virksomheten kontra en med svært sterke administrasjonsbehov?
- Hva slags prisstruktur vil appellere til deg mest fra ditt nåværende perspektiv?
- På samme måte, hvordan vil regional dekning påvirke ditt valg?
- Les denne artikkelen og vurder hva som er dine viktigste hensyn som nåværende eller potensiell bedriftseier når du bestemmer deg for en plattform? https://www.netsolutions.com/insights/how-to-choose-cloud-service-provider/

Ytterligere ressurser: Samoshkin (n. d.), Cloud Industry Forum (2022), Rathore (2022), CloudSigma (2023).

2.4 Tilkoblingstyper for nettverkstjenester og innstilling av dem

2.4.1 Om skyarkitektur

Begrepet "sky" ser ut til å ha sin opprinnelse i nettverksdiagrammer som representerte internett, eller ulike deler av det, som skjematiske skyer. "Cloud computing" ble laget for hva som skjer når applikasjoner og tjenester flyttes inn i internett-"skyen". Cloud computing er ikke noe som plutselig dukket opp over natten; I en eller annen form kan det spores tilbake til en tid da datasystemer eksternt delte databehandlingsressurser og applikasjoner. Mer for tiden refererer cloud computing til de mange forskjellige typer tjenester og applikasjoner som leveres i internettskyen, og det faktum at enhetene som brukes til å få tilgang til disse tjenestene og applikasjonene, i mange tilfeller ikke krever noen spesielle applikasjoner.

Bedrifter søker ofte etter å finne den beste skyløsningen som passer deres unike organisatoriske behov. En stor del av denne beslutningen er å velge en skytjenesteleverandør. Det er fire primære skytjenesteleverandører som kontrollerer flertallet av globale skyressurser. Imidlertid er det andre mindre kjente skyløsninger som tilbyr spesifikke tjenester til nisjemarkeder.

De fire mest brukte skytjenesteleverandørene tilbyr alle SaaS, PaaS, IaaS og mange andre skytjenester på global skala. De største skytjenesteleverandørene inkluderer:

- Googles skytjenester
- Microsoft Azure
- Amazon Web Tjenester (AWS)
- IBM Cloud.

GOOGLE CLOUD SERVICES	MICROSOFT AZURE	AMAZON WEB SERVICES (AWS)	WHAT IT DOES
Google Compute Engine	Azure Virtual Machines	Elastic Compute Cloud (EC2)	Infrastructure as a Service (IaaS)
Google App Engine	Azure Cloud Services	AWS Elastic Beanstalk	Platform as a Service (PaaS)
Google Cloud SQL	Azure SQL Database	Amazon Relational Database Service	Database as a Service (DaaS)
Google Cloud Bigtable	Azure Table Storage	Amazon Dynamo DB	Scalable SQL database services
Google BigQuery	Azure SQL Database	Amazon Redshift	Relational Databases
Google Cloud Functions	Azure Functions	AWS Lambda	Serverless Applications
Google Cloud Datastore	Azure Cosmos DB	Amazon Simple DB	Highly Scalable NoSQL Database Services
Google Storage	Azure Storage	Amazon Simple Storage Service (S3)	Storage of object, blocks and files. Also for cool and cold storage of data.

Figur 2.55. Oversikt over tjenester

Noen andre skyløsninger som tilbyr spesifikke tjenester inkluderer følgende:

- **Heroku:** Stor leverandør av PaaS-skytjenester, inkludert apputvikling, distribusjon, administrasjon og skalering.
- **GitHub:** En stor repositoriumstjeneste for versjonskontroll som brukes til utvikling av samarbeidsapper. Utviklere og ledere kan gjennomgå kode, administrere prosjekter og bygge programvare som felles innsats.
- **QuickBooks Online:** SaaS-versjon av regnskapsprogramvare som tilbys av QuickBooks.
- **BackBlaze:** Tilbyr en skytjeneste for sikkerhetskopiering og gjenoppretting av data for personlig og forretningsbruk.

- ClearDATA: Leverer skyløsninger som er spesifikke for helsesektoren. Utformet for å hjelpe institusjoner med å overholde bransjeforskrifter.
- Salesforce.com: Kjører applikasjonssettet for kundene i en sky, og Force.com- og Vmforce.com-produktene gir utviklere plattformer for å bygge tilpassede skytjenester.
- Dette er bare å skrape overflaten av de ulike skyløsningene som er tilgjengelige. Imidlertid tilbyr disse skytjenesteleverandørene en solid base for å forstå hva slags tjenester som er tilgjengelige.

Egenskaper

Cloud computing har en rekke egenskaper, Hvor de viktigste er:

- Delt infrastruktur Bruker en virtualisert programvaremodell som muliggjør deling av fysiske tjenester, lagring og nettverksfunksjoner. Skyinfrastrukturen, uavhengig av distribusjonsmodell, søker å få mest mulig ut av den tilgjengelige infrastrukturen på tvers av en rekke brukere.
- Dynamisk klargjøring — Åpner for levering av tjenester basert på gjeldende etterspørselskrav. Dette gjøres automatisk ved hjelp av programvareautomatisering, noe som muliggjør utvidelse og sammentrekning av servicekapasitet etter behov. Denne dynamiske skaleringen må gjøres samtidig som du opprettholder høye nivåer av pålitelighet og sikkerhet.
- Nettverkstilgang Må nås over Internett fra et bredt spekter av enheter som PCer, bærbare datamaskiner og mobile enheter, ved hjelp av standardbaserte APIer (for eksempel de som er basert på HTTP). Distribusjoner av tjenester i skyen inkluderer alt fra bruk av forretningsapplikasjoner til den nyeste applikasjonen på de nyeste smarttelefonene.
- Administrert måling — Bruker måling for å administrere og optimalisere tjenesten og for å gi rapporterings- og faktureringsinformasjon. På denne måten faktureres forbrukerne for tjenester etter hvor mye de faktisk har brukt i løpet av faktureringsperioden.
- Kort sagt, cloud computing tillater deling og skalerbar distribusjon av tjenester, etter behov, fra nesten hvor som helst, og som kunden kan faktureres basert på faktisk bruk.

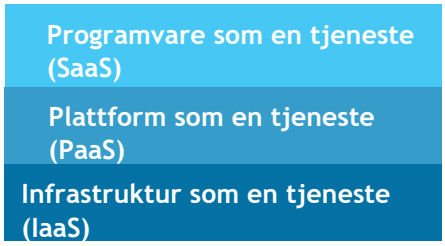
Tjenestemodeller

Når en sky er etablert, kan måten skydatabehandlingstjenestene distribueres på, når det gjelder forretningsmodeller, variere avhengig av krav. De primære tjenestemodellene som tas i bruk (se figur 2.56.) er vanligvis kjent som:

- Programvare som en tjeneste (SaaS) Forbrukere kjøper muligheten til å få tilgang til og bruke en applikasjon eller tjeneste som er vert i skyen. Et benchmark-eksempel på dette er Salesforce.com, som diskutert tidligere, der nødvendig informasjon for samspillet mellom forbrukeren og tjenesten driftes som en del av tjenesten i skyen. Microsoft har også gjort en betydelig investering på dette området, og som en del av cloud computing-alternativet for Microsoft® Office 365 er Office-pakken tilgjengelig som et abonnement gjennom sine skybaserte Online Services.

- Plattform som en tjeneste (PaaS) — Forbrukerne kjøper tilgang til plattformene, slik at de kan distribuere sin egen programvare og applikasjoner i skyen. Operativsystemene og nettverkstilgangen administreres ikke av forbrukeren, og det kan være begrensninger for hvilke applikasjoner som kan distribueres. Eksempler inkluderer Amazon Web Services (AWS), Rackspace og Microsoft Azure.
- Infrastruktur som en tjeneste (IaaS) Forbrukerne kontrollerer og administrerer systemene når det gjelder operativsystemer, applikasjoner, lagring og nettverkstilkobling, men kontrollerer ikke selv skyinfrastrukturen.

Sluttbrukerapplikasjon leveres som en tjeneste. Plattform og infrastruktur er abstrahert, og kan distribueres og administreres med mindre innsats. Applikasjonsplattform som tilpassede applikasjoner og tjenester kan distribueres til. Kan bygges og distribueres rimeligere, selv om tjenester må støttes og administreres. Fysisk infrastruktur er abstrahert for å gi databehandling, lagring og nettverk som en tjeneste, og unngår bekostning og behov for dedikerte systemer.



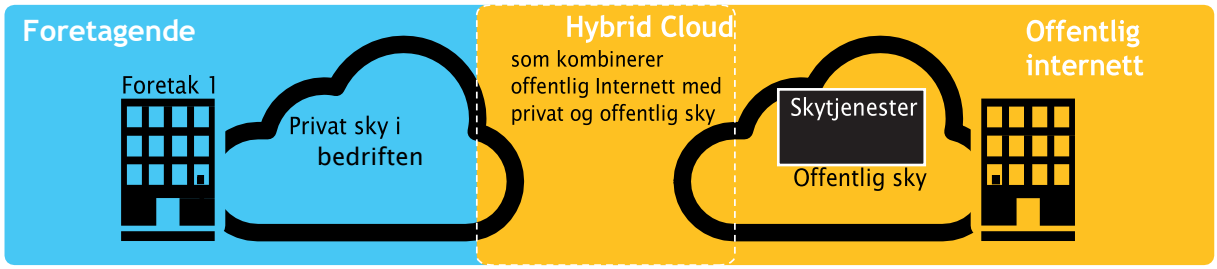
Figur 2.56. Typer tjenestemodeller

Distribusjonsmodeller

Distribusjon av skydatabehandling kan variere avhengig av krav, og følgende fire distribusjonsmodeller er identifisert, hver med sine spesifikke egenskaper som støtter behovene til tjenestene og brukerne av skyene på bestemte måter (se figur 2.57.).

- Privat sky — Skyinfrastrukturen er distribuert og vedlikeholdes og driftes for en bestemt organisasjon. Operasjonen kan være internt eller med en tredjepart i lokalene.
- Community Cloud — Skyinfrastrukturen deles mellom en rekke organisasjoner med lignende interesser og krav. Dette kan bidra til å begrense investeringskostnadene for etableringen ettersom kostnadene deles mellom organisasjonen. Operasjonen kan være internt eller med en tredjepart i lokalene.
- Offentlig sky — Skyinfrastrukturen er tilgjengelig for allmennheten på kommersiell basis av en skytjenesteleverandør. Dette gjør det mulig for en forbruker å utvikle og distribuere en tjeneste i skyen med svært lavere økonomiske utgifter sammenlignet med kapitalutgiftskravene som normalt er knyttet til andre distribusjonsalternativer.
- Hybrid sky — Skyinfrastrukturen består av en rekke skyer av alle typer, men skyene har gjennom sine grensesnitt muligheten til å tillate at data og/eller applikasjoner flyttes fra en sky til en annen. Dette kan være

en kombinasjon av private og offentlige skyer som støtter kravet om å beholde noen data i en organisasjon, og også behovet for å tilby tjenester i skyen.



Figur 2.57. Eksempel på distribusjon av offentlig, privat og hybrid sky

Utfordringer

Følgende er noen av de bemerkelsesverdige utfordringene knyttet til cloud computing, og selv om noen av disse kan føre til en nedgang når du leverer flere tjenester i skyen, kan de fleste også gi muligheter, hvis de løses med tilbørlig forsiktighet og oppmerksomhet i planleggingsstadiene.

- **Sikkerhet og personvern** - Kanskje to av de mer prekære problemene rundt cloud computing er knyttet til lagring og sikring av data og overvåking av bruken av skyen av tjenesteleverandørene. Disse problemene tilskrives vanligvis tregere distribusjon av skytjenester. Disse utfordringene kan for eksempel løses ved å lagre informasjonen internt i organisasjonen, men la den brukes i skyen. For at dette skal skje, må imidlertid sikkerhetsmekanismene mellom organisasjon og skyen være robuste, og en hybrid sky kan støtte en slik distribusjon.
- **Mangel på standarder** — Skyer har dokumenterte grensesnitt; Imidlertid er ingen standarder knyttet til disse, og det er derfor usannsynlig at de fleste skyer vil være interoperable. Open Grid Forum utvikler et Open Cloud Computing Interface for å løse dette problemet, og Open Cloud Consortium jobber med standarder og praksis for databehandling i skyen. Men å holde seg oppdatert på de nyeste standardene etter hvert som de utvikler seg, vil tillate dem å bli utnyttet, hvis det er aktuelt.
- **Kontinuerlig utvikling** – Brukerkravene utvikler seg kontinuerlig, og det samme gjelder kravene til grensesnitt, nettverk og lagring. Dette betyr at en "sky", spesielt en offentlig, ikke forblir statisk og også utvikler seg kontinuerlig.
- **Bekymringer knyttet til overholdelse** – EU har en lovgivende støtte for databeskyttelse i alle medlemsland, men i USA er databeskyttelsen forskjellig og kan variere fra stat til stat. Som med sikkerhet og personvern nevnt tidligere, resulterer disse vanligvis i hybrid skydistribusjon med en sky som lagrer dataene internt i organisasjonen.

2.4.2 Prinsipper for tilkobling til skytilgang

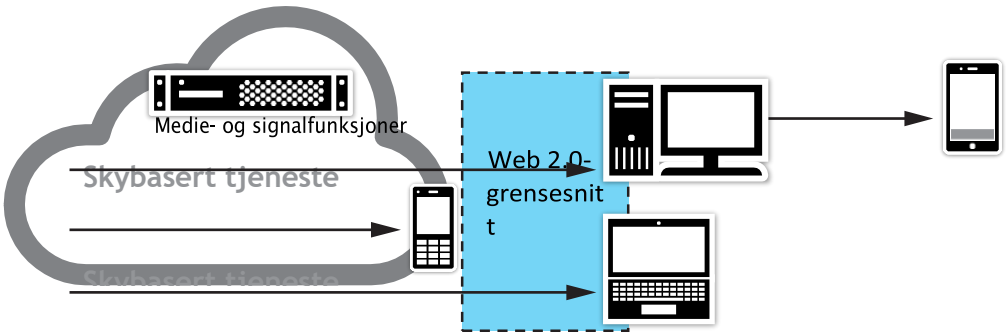
For tjenesteutviklere avhenger tilgjengeliggjøring av tjenester i skyen av tjenestetypen og enheten(e) som brukes til å få tilgang til den. Prosessen kan være så enkel som at en bruker klikker på den nødvendige nettsiden eller kan innebære at en applikasjon bruker en API som får tilgang til tjenestene i skyen.

Tilgang via nettbaserte API-er

Tilgang til kommunikasjonsfunksjoner i et skybasert miljø oppnås gjennom API-er, primært Web 2.0 RESTful API-er, slik at applikasjonsutvikling utenfor skyen kan dra nytte av kommunikasjonsinfrastrukturen i den (se figur 2.58.).

Disse API-ene åpner for en rekke kommunikasjonsmuligheter for skybaserte tjenester, bare begrenset av medie- og signaleringsmulighetene i skyen. Dagens medietjenester muliggjør kommunikasjon og styring av tale og video på tvers av et komplekst spekter av kodeker og transporttyper.

Ved å bruke web-API-ene kan disse kompleksitetene forenkles, og mediet kan leveres til den eksterne enheten på en enklere måte. API-er muliggjør også kommunikasjon av andre tjenester, noe som gir nye muligheter og bidrar til å drive gjennomsnittlig inntekt per bruker (ARPU) og vedleggsrater, spesielt for telekomselskaper.



Figur 2.58. Web 2.0-grensesnitt til skyen

Skalerbarhet for kommunikasjon

For å oppfylle skalerbarhetskravene for skybaserte distribusjoner, bør kommunikasjonsprogramvaren kunne kjøre i virtuelle miljøer. Dette gjør det enkelt å øke og redusere økt-tettheten basert på behovene på det tidspunktet, samtidig som det fysiske ressursbehovet på servere holdes på et minimum.

Valg av alternativ for skytilkobling

Mange nettverkstjenesteleverandører (NSP) har en rekke alternativer når det gjelder skytilkobling, selv om mangel på bransjestandarder og forvirrende terminologi kan gjøre ting vanskelig å forstå.
For ikke så lenge siden var det eneste tilgjengelige alternativet for å koble til en Cloud Service Provider (CSP) å bruke det offentlige Internettet. Men med det raske skiftet til cloud computing begynte kundene raskt å kreve mer - bedre sikkerhet, lavere ventetid, høyere gjennomstrømning og økt pålitelighet.

CSP-er innså snart at bedre ende-til-ende-skyytelse ikke ville være mulig å bruke det offentlige Internett. De forsto også at de ikke hadde ekspertisen eller infrastrukturen til å administrere sammenkobling mellom dusinvis av nettverksleverandører og samlokaliseringsrack i sine egne datasentre.

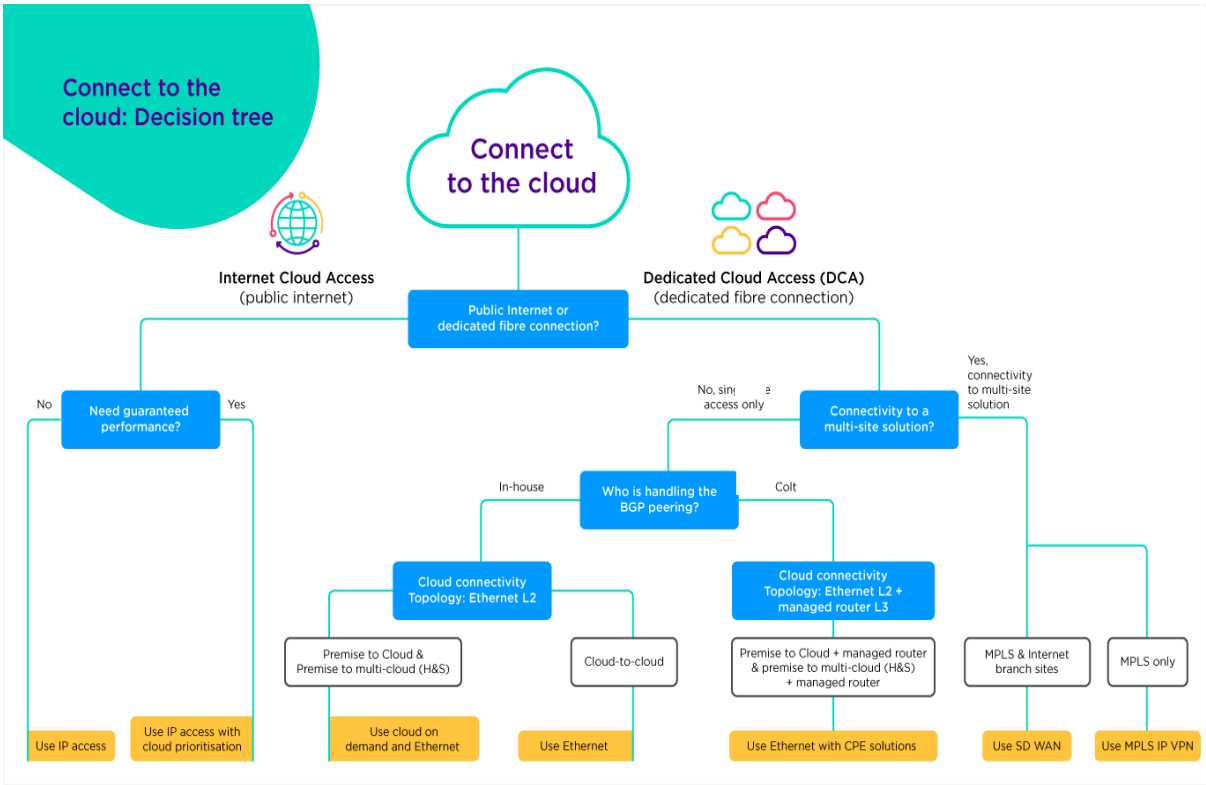
CSP-er innså også raskt at svaret lå i hundrevis av operatørnøytrale datasentre spredt over hele verden, også kjent som Internet Exchange Points (eller IXPs). Alle nettverkstjenesteleverandører var allerede til stede på disse stedene, slik at CSP-er kunne utvide ryggradstilkoblingen for å møte dem der. Dette ga potensialet for en direkte fysisk kobling mellom nettverket av nettverkstjenesteleverandører og nettverket for skytjenesteleverandører (kjent som en kryssforbindelse), omgå det vanlige Internett og gi et pseudo-privat nettverk. Denne sammenkoblingen, kjent som privat nodenettverk, muliggjorde direkte, ende-til-ende-tilkobling og brakte med seg en rekke sikkerhets-, forsinkelse- og ytelsesforbedringer (i tillegg til kostnadseffektivitet for kunder som flytter store datamengder fra skymiljøer til deres lokasjoner).

I dag faller skytilkobling i to kategorier, en som er avhengig av det offentlige Internett, og en annen som bruker privat, dedikert tilkobling. Innenfor disse 2 bøtter er vanligvis 5 forskjellige tilkoblingsmuligheter tilgjengelig (se figur 2.59.).

Internet connectivity	Dedicated connectivity
Public Internet	Ethernet
Public Internet with cloud prioritisation	MPLS IP VPN
	SD WAN

Figur 2.59. Sky-tilkobling

Vi vil lede deg gjennom 5 skytilkoblingsalternativer og forklare fordeler og ulemper med hver, slik at du kan velge den mest passende skytilgangsløsningen for dine behov (se figur 2.60.).



Figur 2.60. Koble til skyen – beslutningstreet

Skytilkobling ved hjelp av det offentlige internett

Uten tvil den billigste og enkleste måten å koble til skyen på er gjennom din standard Internett-tilkobling over det offentlige Internett, noen ganger referert til som IP-tilgang eller IP-transitt.

Bruk av offentlig Internett-tilgang er enkelt å konfigurere og allsidig, siden tilgang til skyen bare er ett av mange brukstilfeller for en standard Internett-tilgangstilkobling. Det gir en kostnadseffektiv tilgangsmetode der du ikke har spesifikke ytelsesbehov.

Tilgang til skyapplikasjoner via det offentlige Internett kan imidlertid også føre til inkonsekvenser i ytelse og økte sikkerhetsrisikoer. Historisk sett ble begrepet IP-transitt brukt for å gjenspeile situasjoner der tilbydere ikke hadde direkte tilgang til destinasjonsnettverket og trengte å overføre over andre nettverk og nettverksleverandører.

Du kan tenke på offentlige Internett-ruter som en motorvei - de er dynamiske og delte, noe som kan føre til overbelastning til tider, og når den mest direkte koblingen ikke er tilgjengelig, rutes data gjennom det nest

beste alternativet, som du ikke har kontroll over, noe som resulterer i pakketap og økt ventetid (forsinkelser). I tillegg skaper flere overleveringer mellom Internett-leverandører ustabilitet i forbindelsen og økt risiko.
I hovedsak jo flere tilstedeværelsespunkt (PoPs) og rutere som er involvert i å levere dataene dine til den endelige destinasjonen, jo flere poeng med potensiell feil og et bredere overflateområde for sikkerhetsangrep. Til tross for dette har veksten av skytilkobling via offentlig Internett ikke vist noen tegn til å bremse ned. Det offentlige Internett er fortsatt den desidert vanligste måten å få tilgang til skyen på (se figur 2.61.).

Advantages	Disadvantages
Best for single locations	A best-effort service not suited for critical applications
Cost-effective for low and medium data transfer volumes	Shared and dynamic routes mean no performance optimisation or guaranteed performance
Suitable for most topologies (premise/wan to single cloud, premise/wan to multi-cloud)	Not suitable for cloud-to-cloud connectivity
Use your existing business-as-usual internet connection	Becomes expensive for higher data transfer rates due to per Gigabyte out billing (egress)
Easy to get up and running, no need for a dedicated circuit	Exposed to security risks, such as DoS and DDoS attacks against routers and links
On demand delivery and scaling typically available	The least secure connectivity option

Figur 2.61. Skytilkobling ved hjelp av det offentlige internett (fordeler og ulemper)

Skytilkobling ved hjelp av offentlig Internett- og skyprioritering

Internett-tilkobling med skyprioritering gjør at du dynamisk kan reservere en del av den vanlige Internett-båndbredden for utvalgte skyprogrammer. Trafikkprioritering er effektiv for både innkommende og utgående trafikk, noe som muliggjør en konsekvent, SLA-støttet brukeropplevelse spesielt for trafikken din til skyen.

Skyprioritering tilbys av nettverkstjenesteleverandører som har direkte nodenettverk med skyleverandører, for eksempel Microsoft. Microsoft Azure Peering Services (forkortet MAPS) gir for eksempel sluttbrukernes direkte tilgang til Microsoft-skytjenester gjennom sertifiserte nettverksleverandører.

Når den er på plass, forblir skytrafikken din helt på leverandørens nettverk, omgår det offentlige Internett og unngår andre mellomliggende Internett-leverandører.

Skyprioritering kombinerer fordelene med optimalisert ruting og direkte nodenettverkinfrastruktur med trafikkprioritering den siste milen, mellom kundens ruter og tilbyderens nettverkskant. Fordeler og ulemper vist i figur 2.62.

Advantages	Disadvantages
An add-on to standard Internet access services	Offerings are dependent on your connectivity and cloud providers
Consistent and guaranteed SLA-backed performance to the closest peering point	Layer 3 access only
Dynamically reserved bandwidth for cloud applications	No dedicated connection
Works for both incoming and outgoing bandwidth	
Optimised routing selects the shortest path to the cloud network edge	
Avoids network contention and unpredictable routing changes	
30 milli second Round Trip Delay (RTD)	
Traffic congestion control *	

** only available from some MAPS providers*

Figur 2.62. Skytilkobling ved hjelp av offentlig Internett og skyprioritering (fordeler og ulemper)

Direkte Ethernet-skytilkobling

Dedikert tilkobling gjennom Ethernet-tilkoblingstjenester er den raskeste og sikreste ruten for skytilkobling, og den første av Internett-bypass-løsningene. Det er resultatet av at tjenesteleverandører, som Amazon, Microsoft, Google, Oracle og IBM, samarbeider med nettverkstjenesteleverandører for å forbedre ende-til-ende skytilkobling og automatiseringsfunksjoner - uten å berøre Internett. Sluttbrukere er sannsynligvis allerede kjent med navnene på disse CSPs direkte sammenkoblingsprogrammer - som AWS Direct Connect, Microsoft ExpressRoute og Google Cloud Interconnect - som muliggjør ende-til-ende sikker tilkobling gjennom en nettverkstjenesteleverandør mot kundens plassering.

Direkte Ethernet-tilkobling til skyen gjør ytelse, tjenestekvalitet og sikkerhetsproblemer foreldet. Den leveres av skyramper på datasentre der skytjenesteleverandøren er til stede. Dette kobler lokalene eller fasilitetene dine gjennom en NSP til skyleverandøren via en dedikert lag 2-kobling.

Direkte skytilkobling gir den sikre, ende-til-ende-tilkoblingen med høy ytelse som trengs for å kjøre kritiske programmer som ikke kan måle seg med når du bare bruker Internett. Skytjenesteleverandører krever vanligvis dataoverføringsgebyrer - som er forskjellige når du kobler til skyen via direkte Ethernet-tilkobling kontra via Internett, så direkte tilkobling kan være spesielt kostnadseffektiv hvis du sannsynligvis vil transportere store mengder data ut fra skymiljøet ditt (kjent som "utgang") mot posisjonen din.

Advantages	Disadvantages
Supports all topologies (Premise to cloud, premise to multi-cloud and cloud to cloud)	Only suitable for a single site (not multisite/WAN connectivity)
Bandwidth services up to 100Gbps available	Requires a dedicated circuit
Bandwidth is fully dedicated and guaranteed end-to-end	Customer to handle BGP peering
On demand delivery and scaling typically available	By default a layer 2 service, some NSP's provide managed router (L3)
End to end connectivity SLA with deterministic latency and performance	
Very suited and cost efficient for higher data transfer - due to lower price per Gigabyte (egress) out billing vs through the Internet	
Not subject to DDOS attacks as traffic bypasses the public Internet	

Figur 2.63. Direkte Ethernet-skytilkobling (fordeler og ulemper)

Multiprotocol Label Switching (MPLS) IP VPN skytilkobling

Integrering av skytilkobling i en IP-VPN (også kjent som IP-VPN cloud connect eller MPLS-WAN-teknologi) er en skalerbar og kostnadseffektiv måte å få tilgang til skytjenester på.

MPLS IP-VPN gir direkte, høy båndbredde og sikker skytilkobling til skytjenesteleverandører. Det er egnet for kunder som krever sikker tilgang til skyen på tvers av flere nettsteder, og har tradisjonelt vært en vanlig måte for bedrifter å koble seg til skyleverandører.

Skytilkoblingen er direkte integrert i IP VPN, slik at den er helt privat, uten avhengighet av Internett. Skylokasjonene er integrert i det private WAN og effektivt sett på som et annet nettsted (eller nettsteder) på IP-VPN, noe som betyr at det ikke er behov for å redesigne store bedriftsnettverk. Ulike kundelokasjoner i IP-VPN deler deretter tilkoblingen for å få tilgang til ressursene sine i skyen.

Advantages	Disadvantages
Very suitable for integration in existing and new MPLS IP-VPN networks	MPLS only, no Internet Branch sites
Highly secure, part of private IP-VPN	Layer 3 connectivity
No need to redesign large corporate networks	Dedicated connection required
Fully integrated in IP-VPN (any-to-any), avoids the need to backhaul traffic	Can increase latency – depends on where branch sites are located
Cost-effective as multiple locations on the IP-VPN share the connectivity toward the cloud	
Support different topologies: Single Cloud, Multi-Cloud and Cloud-to-Cloud	

Figur 2.64. MPLS IP VPN cloud connect (fordeler og ulemper)

SD WAN-skytilkobling

SD WAN (noen ganger kalt SDWAN, SD WAN Cloud Access eller SD WAN Multi-Cloud) kan koble din programvaredefinerte WAN-infrastruktur til flere skytjenesteleverandører (for eksempel AWS, Microsoft

Azure og Google Cloud) for å muliggjøre direkte, høy ytelse og sikker tilkobling til flere skyer. Hvert avdelingskontor drar nytte av sømløs ende-til-ende-tilkobling til dine offentlige skyleverandører.

For kostnadseffektiv, direkte tilkobling til flere skymiljøer, er SD WAN sannsynligvis den optimale løsningen.

SD WAN tilbyr sofistikerte og omfattende tilkoblingsmuligheter, med funksjoner som prioritering, optimalisering, sikkerhet, analyse, automatisert klargjøring og distribusjon. Den samler en enkelt sammenhengende visning av bedriftsnettverket, og knytter sammen WAN-nettsteder, IaaS/SaaS-sky og tilkobling til avdelingsområder, vanligvis alt innenfor en enkelt nettportal. Kombinert med on-demand-funksjoner som zero touch site provisioning og båndbreddeoppgraderinger i sanntid, er SD WAN en ekstremt kraftig løsning.

Før SD WAN ble trafikken vanligvis trukket tilbake til et sentralt sted eller regionalt knutepunkt der en fysisk maskinvarestakk ga funksjonalitet som var kostnadskrevende å distribuere på satellittsteder (for eksempel sikkerhet og analyse). SD WAN gjør det nå mulig å distribuere denne funksjonaliteten i programvare på en felles maskinvareplattform. Disse programvarestakkene består av ulike programvarefunksjoner som kan lastes dynamisk og distribueres på en modulær måte med en rekke funksjoner, inkludert:

- Nettverk og ruting
- Analytics
- Sikkerhet
- Trafikkoptimalisering
- Ekstern tilgang
- og mer.

Ved å knytte sammen WAN-nettsteder og skyinfrastruktur kan SD WAN levere ende-til-ende-sikkerhet, ytelse og synlighet.

SD WAN bygger på MPLS IP VPN ovenfor, og tilbyr privat tilkobling til flere skyleverandører i en enkelt løsning, kombinert med ende-til-ende-ytelse støttet av en SLA, ende-til-ende-sikkerhet og ende-til-ende-analyse.

Advantages	Disadvantages
The best way to manage multi-cloud infrastructures (MPLS and Internet branch sites)	Can require significant network changes and redesign to leverage all the benefits
Completely avoids the need to backhaul traffic from a brand site to a CSP or data centre	Newer services such as on demand capabilities may be limited
Bandwidth is fully dedicated and guaranteed end-to-end	Check support for your specific cloud provider (CSP) requirements
Automatic provisioning and deployment	Check support and roadmap for features and functionality such as such as application optimisation, analytics, SASE and more
Dynamic path selection - intelligent and dynamic routing to the best available path	Can increase latency – depends on where branch sites are located
Additional security features like FW/NAT to support the CSP public domain	
End-to-end visibility and management of the entire enterprise network	
Supports all topologies - WAN to cloud, WAN to multi-cloud and cloud to Cloud	
Also supports Internet only branch sites connecting directly to CSP through SD-WAN	

Figur 2.65. SD WAN cloud connect (fordeler og ulemper)

Det finnes ingen «one-size-fits-all»-løsning for bedrifter når de kobler seg til skyen. Her er de ti viktigste spørsmålene og hensynene for å sikre at du forblir fremtidssikret av en ny leverandør:

1. Hvilket nivå av partnerskap har du med de store skyleverandørene?
2. Hvor mange tilstedeværelsespunkter i offentlige skyer har dere?
3. Hvor mange datasentre er for øyeblikket koblet til nettverket ditt?
4. Hvor mange kontorer er for øyeblikket koblet til nettverket ditt?
5. Tilbyr dere muligheter på forespørsel via en selvbetjent programvareportal?
6. Er datasenteret og skytjenesteleverandøren nøytral?

7. Hvem eier fibernettet ditt - er det privateid eller leid fra en 3. part
8. Tilbyr dere ende-til-ende-tilkobling, inkludert den siste milen?
9. Tilbyr dere garanterte serviceavtaler inkludert for ventetid, pakketap og gjennomstrømning?
10. Hvilke båndbredder støttes for skytilkobling?

2.4.3 Oppsett av skynettverk

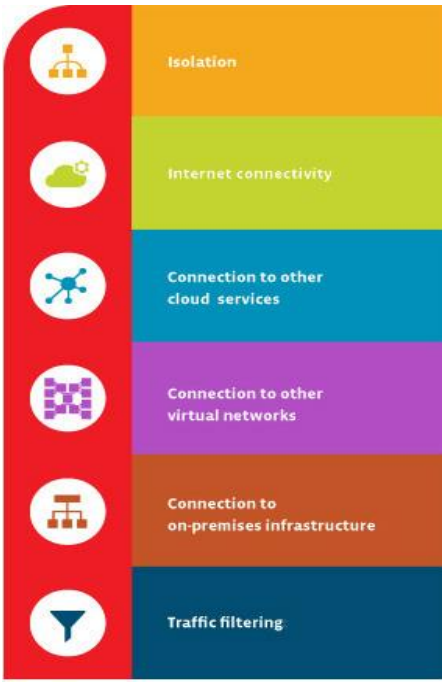
Selv om det ofte går ubemerket hen av den gjennomsnittlige brukeren, implementeres nettverk for å isolere data fra omverdenen. Organisasjoner er avhengige av nettverk for å koble til enhetene sine og integrere systemene sine på tvers av geografiske barrierer, samtidig som de sikrer trygg passasje for informasjon. Denne hurtigveiledningen veileder deg gjennom det grunnleggende om konfigurering av skynettverket.

Virtuelt nettverk

Virtuelle nettverk kan betraktes som separate nettverk i et større nettverk. Administratorer kan opprette et eget nettverkssegment som består av en rekke delnett (eller et enkelt delnett) og kontrollere trafikk som flyter gjennom skynettverket. Avhengig av forretningsbehovene dine kan du implementere nettverket ditt ved hjelp av skyteknologi fra en skytjenesteleverandør (CSP).

Hovedforskjellen for skyadministratorer og arkitekter når det gjelder å designe skynettverksløsninger, er mengden kontroll som trengs for å ha over maskinvaren. Når du implementerer skynettverk med en CSP, har du liten kontroll over - og sannsynligvis lite kunnskap om - utformingen av CSPs nettverk. På grunn av denne begrensningen er virtuelle nettverk ofte det beste valget når du vil gi sikker nettverksisolasjon.

Med en skyløsning er disse virtuelle nettverkene kjent som VNets eller Virtual Private Clouds (VPC). Disse fungerer som en representasjon av et nettverk i skyen, og gir deg et skynettverk.
Virtuelle nettverk gir følgende fordeler:



Figur 2.66. Virtuelle nettverk

- Isolasjon

Du kan holde nettverk isolert fra hverandre for å sikre sikkerhet og for utvikling, kvalitetssikring og distribusjon av skynettverk.

- Internett-tilkobling

Hvert virtuelle nettverk kan konfigureres til å få tilgang til eller nekte tilgang til internett, eller til å begrense tilgangen til bestemte destinasjoner på internett om nødvendig.

- Tilkobling til andre skytjenester

Virtuelle nettverk trenger ofte en tilkobling til CSP-tjenester. Dette gjør at nettverket kan bruke tjenester som tilbys av CSP. Leverandører tillater vanligvis konfigurasjon av rutetabeller, domenenavnoppløsning, brannmur og relaterte elementer for å administrere tilkoblingene til de virtuelle nettverkene dine.

- Tilkobling til andre virtuelle nettverk

Dette lar deg koble sammen de virtuelle nettverkene dine når det er nødvendig, samtidig som du opprettholder kontrollen over tilkoblingene.

- Tilkobling til lokal infrastruktur

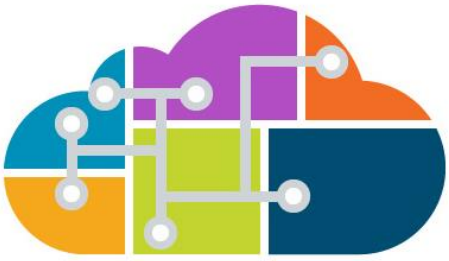
En del av fleksibiliteten til et virtuelt nettverk er muligheten til å kontrollere tilkoblinger. Du kan koble det virtuelle nettverket til lokale systemer. Ofte er denne typen konfigurasjon for sluttbrukere å få tilgang til et sikkert privat skynettverk eller gjøres som en del av en hybrid skyimplementering.

- Filtrering av trafikk

De fleste sikre tilkoblinger involverer filtrering. Normalt innebærer dette filtrering av elementer etter kilde-IP-adresse og port, destinasjons-IP-adresse og port, og bestemt protokoll. Dette gir cloud computing-ingeniører økt kontroll over kommunikasjonen som skjer på nettverket ditt.

Byggeklosser i skynettverket

Som skyadministrator eller cloud computing-ingeniør vil din evne til å opprette et virtuelt nettverk vanligvis være avhengig av programvare for virtuell maskin eller et skynettverk levert av en CSP. Programvare for virtuell maskin gjør det mulig for skyadministratorer å utpeke og konfigurere virtuelle nettverksparametere knyttet til en verts fysiske nettverkskort (NIC). Når du konfigurerer flere verter til å operere med de samme parameterne, legger du til disse vertene i det virtuelle nettverket. Virtuelle nettverk må ha følgende komponenter:



Figur 2.67. Byggeklosser i skynettverket

- **Virtuell bryter**

Virtuelle svitsjer gir deg muligheten til å opprette segmenter på nettverket og koble disse komponentene sammen. Du kan koble én eller flere virtuelle maskiner til en virtuell svitsj.

- **Virtuell bro**

Denne komponenten lar deg koble virtuelle maskiner til LAN som brukes av vertsmaskinen. Den virtuelle broen kobler nettverkskortet på den virtuelle maskinen til det fysiske nettverkskortet på vertsdatamaskinen. Flere virtuelle broer kan konfigureres til å koble til flere fysiske NIC-er.

- **Virtuell vertsadapter**

Adapteren gjør det mulig for de virtuelle maskinene dine å kommunisere med verten. Virtuelle vertsadaptere er vanlige i bare vert og NAT-konfigurasjoner (Network Address Translation). Disse kan ikke koble til et eksternt nettverk uten en proxy-server.

- **NAT-tjeneste**

NAT-tjenester lar flere enheter i skynettverket koble til Internett.

- **DHCP-tjener**

DHCP-serveren tildeler IP-adresser til virtuelle maskiner og verter. Dette gjelder bare vert- og NAT-konfigurasjoner.

- **Ethernet-adapter**

Dette er et fysisk nettverkskort installert på verter som kobler til nettverket.

Mange CSP-er tilbyr skytjenester som gjør det enklere å konfigurere virtuelle nettverk og skynettverk. Med skynettverk konfigurerer du det virtuelle nettverket og legger til ressursene dine i dem, i stedet for å konfigurere dem på nivå med den virtuelle maskinen. Skynettverk tilbyr også vanligvis funksjoner for å forenkle overvåking, administrasjon, tilkoblinger og sikkerhet.

Alternativer for nettverkskonfigurasjon for oppmåling

Hvis du vil bruke et virtuelt nettverk, må du også konfigurere følgende komponenter:

Figur 2.68. Alternativer for nettverkskonfigurasjon for oppmåling

- Subnett

Subnett er en nødvendig del av et virtuelt nettverk. Du trenger TCP/IP-delnett, som angir adresser som brukes på nettverket. Offentlige og private adresseområder brukes ofte. Når det ikke er mulig, tildeles adresser ofte av CSP-er. Virtuelle nettverk kan segmenteres i ett eller flere delnett.

- Rutere eller rutetabeller

For alle nettverk må du konfigurere rutere eller rutetabeller på en hvilken som helst virtuell maskin som er koblet til nettverket, slik at pakker kan rutes på riktig måte.

- DNS

DNS-serveradresser må oppgis, enten tilordnet av deg eller CSP-en din.

- CSP-region eller -soner

Virtuelle nettverk som opererer i forskjellige CSP-regioner må spesifiseres. Hvis du gjør det, kan du også koble til virtuelle nettverk i forskjellige regioner. Om nødvendig kan du også konfigurere isolering mellom områder.

- Trafikk-filtrering

Konfigurering av trafikkfiltrene til spesifikasjonene til sikkerhetsprotokollene dine vil bare tillate godkjent trafikk å passere gjennom nettverket ditt. Filtre kan brukes på NIC i virtuelle maskiner, til et delnett eller til en skytjeneste. Når det er nødvendig, vil du gjøre dette med et virtuelt nettverksapparat.

Tips om utforming av skynettverk

Når du utformer skynettverk, bør du vurdere følgende:

- Når du designer skynettverket ditt, bør du ta deg tid til å sammenligne virtuelle nettverkstjenester som tilbys av skyleverandører. Et vertsbasert skynettverk kan være den eneste måten du kan opprette virtuelle nettverk slik du vil ha dem. Ofte er disse skynettverkene enklere å konfigurere og administrere.
- Hvis du planlegger å filtrere trafikk (noe de fleste selskaper burde!), Planlegg testing av filteret i distribusjonen for å unngå fremtidige brukerklager på grunn av blokkert trafikk.
- Hvis du velger å velge en CSP, må du samarbeide med personalet deres for å konfigurere skynettverkskomponentene dine, for eksempel rutetabeller, virtuelle nettverksapparater og delnett. Spar deg selv litt bryderi.

Cloud Networks porter og protokoll

Et av de viktigste skrittene du må ta for å sikre skynettverket ditt, er å bore ned i det nitty gritty for å avdekke hvilke mennesker, tjenester og teknologier som trenger tilgang til nettverket. Porter er en viktig del av skynettverket ditt. Porten er endepunktet for tilkoblingen.

Brukere kobler seg til skynettverket via en utpekingsport. Alle porter er tildelt et nummer fra 0 til 65 535. IANA (Internet Assigned Numbers Authority) deler portnumre inn i tre porter vist i figur 2.69., basert på numrene. TCP- og UDP-porter tilordnes basert på disse områdene. Hackere går ofte etter kjente porter, men har også vært kjent for å målrette mot åpne registrerte eller dynamiske porter.

De tre portene er:

- Kjente porter

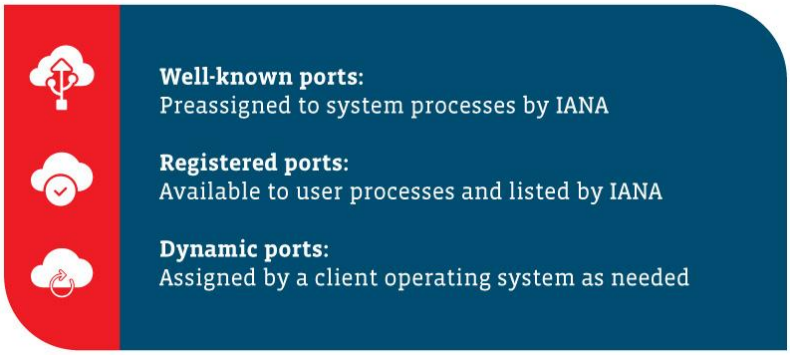
Disse er forhåndstilordnet systemprosesser av IANA, og inkluderer 0 til 1,023 og er mest utsatt for angrep.

- Registrerte porter

Tilgjengelig for brukerprosesser og oppført av IANA, går disse registrerte portene fra 1,024 til 49,151 og er kjent for å være for systemspesifikke for direkte mål av hackere. Imidlertid skanner hackere noen ganger etter åpne porter i dette området. Ikke snu ryggen til, men du kan avverge blikket av og til.

- Dynamiske eller private porter

Tilordnet av et klientoperativsystem etter behov, dette er portene nummerert fra 49,152 til 65,535. Dynamiske porter er i stadig endring (dermed navnet dynamisk), så det er vanskelig å angripe spesifikke tall direkte. Men igjen har hackere vært kjent for å skanne etter åpne porter. Når det gjelder å se etter hackere, kan du kanskje snu ryggen til dynamiske eller private porter, men ikke for lenge!



Figur 2.69. Dynamiske eller private porter

Så, hva brukes disse portene til? Her er en liste over noen av de vanligste standard nettverksportene som brukes i teknologiverdenen:

- 21 FTP (File Transfer Protocol)
- 22 SSH (sikkert skall)
- 25 SMTP (enkel e-postoverføringsprotokoll)
- 53 DNS (domenenavnsystem)
- 80 HTTP (Hypertext Transfer Protocol)
- 110 POP3 (postkontorprotokoll)
- 139 NetBIOS-økttjeneste
- 143 IMAP (protokoll for tilgang til Internett-meldinger)
- 443 HTTPS (Hypertext Transfer Protocol Secure)
- 3389 RDP (protokoll for eksternt skrivebord).

Vedlikehold av skynettverket ditt

Tjenester og apper som flyter mellom skyen, ligner på mange måter tjenestene og appene som forblir forankret i den lokale infrastrukturen. Ta for eksempel skybaserte nettapper og katalogtjenester. Mange vil bruke de samme portene og protokollene som brukes av deres lokale motstykker. Administrasjonsverktøy, enten CSP-baserte, tredjeparts eller de som er bygget av IT-teamet ditt, vil også benytte port- og protokollkrav.

Hvis du bestemmer deg for å hoppe fra bakken til skyen, må du gjennomgå portene dine for å finne ut hva som må være basert i skyen og hva som må forbli plassert på din egen infrastruktur. Ta en nærmere titt på hva som trenger internettilgang, for å kommunisere med eksterne tjenester eller apper, og hvilken type tilgang som kreves fra skyen.

Når du har begrenset det, kan du konfigurere brannmurer og angi de nødvendige filtrene for å sikre at skynettverket ditt forblir sikkert. Når du jobber med å distribuere skynettverket, må du sørge for å konsultere følgende ressurser:

Figur 2.70. Vedlikehold av skynettverket ditt

- Veiledninger for konfigurasjon av apper og tjenester for å identifisere de nødvendige portene og protokollene hver enkelt bruker.
- CSP-sikkerhets- og distribusjonsveiledninger eller white papers for å finne portene og protokollene du trenger for å få tilgang til skytjenester som nettsteder, databaser, katalogtjenester og så videre.
- Distribusjonsveiledninger fra tredjeparter som ligner på skynettverket du implementerer.
- Din egen (ja, din egen) dokumentasjon for å referere til brannmuren, ruting og annen relatert informasjon som kan hjelpe deg med å forstå din egen port- og protokollbruk. Det vil være vanskelig å implementere en vellykket skydistribusjon hvis du ikke aner hvor du hopper fra.
- Hvis skjebnene forbyr deg å avdekke hvilke porter og protokoller som brukes av et eldre program som du vil flytte til skyen, vil du kanskje samle noen nyttige verktøy som en portskanner eller protokollanalysator for å låse opp de bevoktede hemmelighetene til forgjengerne dine.
- Før du starter et skynettverk, ta en fintannet kam gjennom alle appene og tjenestene dine for å sikre at alle porter og protokoller tråkker linjen.

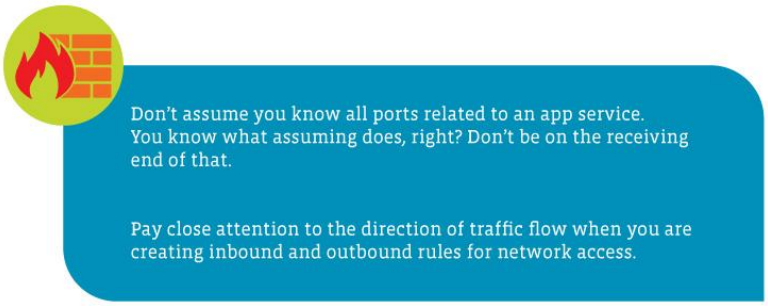
Bestem tildeling av tilgang til skynettverket

Før du gir disse magiske inngangspassene og gir tilgang til skynettverket ditt, bør du vurdere disse retningslinjene i tillegg til informasjonen som allerede er oppgitt:

- Ikke anta at du kjenner alle porter relatert til en apptjeneste. Du vet hva antagelse gjør, ikke sant? Ikke vær på mottakersiden av det.
- Vær nøye med retningen på trafikkflyten når du oppretter innkommende og utgående regler for

nettverkstilgang.

Skynettverk er fortsatt en ny teknologi, som viser mange muligheter for fremtiden for IT.



Figur 2.71. Bestem tildeling av tilgang til skynettverket

2.5 Skysystemadministrasjon (overvåkings- og varslingstjeneste)

Vanskelighetsgrad: Lett

Fullføringsperiode:

Mål

Etter å ha lest materialet, vil leseren forstå begrepet Cloud Management, Cloud Management systemer og overvåkingsverktøy. Du vil også kjenne til hovedmålene og egenskapene til Cloud Management, plattformer, verktøy og leverandører.

Figur 2.72. Administrasjon av skysystemer

Læringsmål

Etter å ha fullført denne søknaden, vil du kunne:

- vite hva Cloud Management refererer til
- Hvordan Cloud Management fungerer
- viktigheten av Cloud Management
- Mål og egenskaper for Cloud Management
- Vite hva de 4 typene Cloud Management er
- Vite hva skyovervåking refererer til
- Utfordringene med skyovervåking
- Analyse av skyadministrasjonsplattformer, verktøy og leverandører.

Introduksjon av Cloud Management og Cloud Management Systems

Hva er Cloud Management?

Skyadministrasjon refererer til utøvelse av kontroll over offentlige, private eller hybride skyinfrastrukturressurser og -tjenester. En godt utformet strategi for skyadministrasjon kan hjelpe IT-eksperter med å kontrollere dynamiske og skalerbare databehandlingsmiljøer. Skyadministrasjon er **prosessen med å overvåke og maksimere effektiviteten i bruken av en eller flere private eller offentlige skyer.** Organisasjoner bruker vanligvis en skyadministrasjonsplattform for å administrere skybruk. Videre er Cloud Management en **metode for å gjennomgå, observere og administrere den operative arbeidsflyten i en skybasert IT-infrastruktur**. Manuelle eller automatiserte administrasjonsteknikker bekrefter tilgjengeligheten og ytelsen til nettsteder, servere, applikasjoner og annen skyinfrastruktur.

Hvorfor brukes Cloud Management?

Organisasjoner distribuerer i økende grad bedriftsapplikasjoner til skyen for å redusere de høye forhåndsinvesteringene de ellers måtte gjøre for infrastruktur på stedet. Offentlige skymiljøer gir datakraft og datalagring på forespørsel som er i samsvar med den voksende, varierende etterspørselen etter data og tjenester. Gjennom administrasjon av skytjenester overvåker administratorer skyaktiviteter som spenner fra ressursdistribusjon og utnyttelse til livssyklusadministrasjon av ressurser, dataintegrasjon og katastrofegjenoppretting.

Hvordan fungerer Cloud Management?

Oppsummering av alt ovenfor, Cloud management er en disiplin som tilrettelegges av verktøy og programvare. For å realisere kontrollen og synligheten som kreves for effektiv skyadministrasjon, bør bedrifter eller andre interesserte parter se sin hybride IT-infrastruktur gjennom en sammensatt plattform som henter relevante data fra alle organisasjonens skybaserte og tradisjonelle lokale systemer.

Plattformer for skyadministrasjon hjelper IT-team med å sikre og optimalisere skyinfrastrukturen, inkludert alle applikasjoner og data som ligger på den. Administratorer kan administrere samsvar, sette opp overvåking i sanntid og forhindre nettangrep og databrudd.

Så hvordan fungerer det? Vanligvis installeres et skyadministrasjonssystem på en nevnt målrettet sky. Etter å ha fanget informasjon om aktivitet og ytelse, sendes en analyse til et nettbasert dashbord. Der kan administratorer observere og reagere deretter. Hvis det oppstår et problem, kan administratorer dele kommentarer tilbake til skyen via skyadministrasjonsplattformen.

Viktigheten av Cloud Management

Bedrifter / organisasjoner er mer sannsynlig å forbedre cloud computing ytelse, pålitelighet, kostnadsbegrensning og miljømessig bærekraft. Administrasjon av applikasjoner inneholder gjenntagende oppgaver som gjennom Cloud Management-servere og push-kode kan klargjøres automatisk via API-er i stedet for manuell administrasjon. Cloud Management kan spille en viktig rolle i å håndtere sikkerhetsstatusen og sårbarheten til IT-eiendeler.

Mål og egenskaper for Cloud Management

Uten tvil er den største utfordringen for skyadministrasjon skyspredning (skyspredning er ukontrollert spredning av en organisasjons skyinstanser, tjenester eller leverandører) - IT-ansatte mister oversikten over skyressurser, som deretter multipliserer ukontrollert i hele organisasjonen. Skyspredning kan øke kostnadene og skape sikkerhets- og administrasjonsproblemer, så IT-bedrifter trenger styringspolicyer og rollebaserte tilgangskontroller på plass.

Viktige områder innen skyadministrasjon inkluderer automatiserte og orkestrerte forekomster og konfigurasjoner, sikker tilgang og overholdelse av retningslinjer og overvåking på alle nivåer – alt gjort så kostnadseffektivt som mulig.

Figur 2.73. Komponenter for skyadministrasjon

Plattformer for skyadministrasjon gir en felles visning på tvers av alle skyressurser for å overvåke både interne og eksterne skytjenester. Administrasjonsplattformverktøy kan hjelpe alle individer som berører et programs livssyklus. Regelmessige revisjoner kan holde ressursene i sjakk. Til slutt bør du vurdere tredjepartsverktøy for å finjustere bedriftens bruk, ytelse, kostnader og forretningsfordeler.

Beregninger må utlignes for å bidra til å identifisere trender og gi veiledning om hva brukeren vil måle og spore over tid. Det er mange potensielle datapunkter, men hver bedrift / interessert part bør velge de som betyr mest for deres virksomhet / organisasjon / prosjekt.

Mer analytisk må følgende vurderes:

- Data om bruken av en databehandlingsinstanss volum og ytelse (prosessor, minne, disk osv.) gir innsikt i programmets generelle helse.
- Lagringsforbruk refererer til lagring knyttet til databehandlingsinstansene.
- Lastbalanseringstjenester distribuerer innkommende nettverkstrafikk.
- Databaseinstanser hjelper til med å samle og analysere data.
- Cache-instanser bruker minne til å holde ofte brukte data og dermed unngå behovet for å bruke tregere medier, for eksempel disklagring.
- Funksjoner, også kalt serverløse databehandlingstjenester, brukes til å klargjøre arbeidsbelastninger og unngå behovet for å levere og betale for databehandlingsinstanser. Skyleverandøren driver tjenesten som laster, utfører og laster ut funksjonen når den oppfyller utløserparametere.

Typer skyadministrasjon

Det er fire (4) hovedtyper av databehandling som er kategorisert til **private skyer, offentlige skyer, hybride skyer og multiskyer.**

Mer analytisk:

- **Private skyer:** er definert som databehandlingstjenester som tilbys enten over Internett eller et privat internt nettverk, og bare til utvalgte brukere i stedet for allmennheten. Privat databehandling i skyen, som også kalles en intern sky eller bedriftssky, gir bedrifter/organisasjoner mange av fordelene med en offentlig sky – inkludert selvbetjening, skalerbarhet og elastisitet – med den ekstra kontrollen og tilpasningen som er tilgjengelig fra dedikerte ressurser over en databehandlingsinfrastruktur som driftes lokalt. Private skyer leverer et høyere nivå av sikkerhet og personvern gjennom både bedriftsbrannmurer og intern hosting for å sikre at operasjoner og sensitive data ikke er tilgjengelige for tredjepartsleverandører.
- **Offentlige skyer:** IT-modeller der leverandører av offentlige skytjenester gjør databehandlingstjenester – inkludert databehandling og lagring, utviklings- og distribusjonsmiljøer og programmer – tilgjengelige ved behov for organisasjoner og enkeltpersoner over det offentlige Internett.
- **Hybride skyer:** noen ganger kalt en skyhybrid – er et databehandlingsmiljø som kombinerer et lokalt datasenter (også kalt en privat sky) med en offentlig sky, slik at data og programmer kan deles mellom dem.

- Multi-clouds: et selskaps/ organisasjons bruk av flere cloud computing og lagringstjenester fra forskjellige leverandører i en enkelt heterogen arkitektur for å forbedre skyinfrastrukturens evner og kostnader. Det refererer også til distribusjon av skyressurser, programvare, applikasjoner, etc. på tvers av flere skyvertsmiljøer.

Verktøy for skyadministrasjon og overvåking

Skyovervåking er en **metode for å gjennomgå, observere og administrere den operative arbeidsflyten i en skybasert IT-infrastruktur**. Manuelle eller automatiserte administrasjonsteknikker bekrefter tilgjengeligheten og ytelsen til nettsteder, servere, applikasjoner og annen skyinfrastruktur.
Skyovervåking måler betingelsene for en arbeidsbelastning og de ulike kvantifiserbare parameterne som er relatert til den generelle skydriften. Resultatene overvåkes i spesifikke, granulære data, men dataene mangler ofte kontekst.

Cloud observerbarhet er en prosess som ligner på skyovervåking ved at den hjelper til med å vurdere skyhelsen. Observerbarhet handler mindre om beregninger enn hva som kan hentes fra en arbeidsbelastning basert på dens eksternt synlige egenskaper. Det er to aspekter ved skyobserverbarhet: metodikk og driftstilstand. Metodikk fokuserer på detaljer, for eksempel beregninger, sporing og logganalyse. Driftstilstand er avhengig av sporing og adresserer tilstandsidentifikasjon og hendelsesforhold, hvorav sistnevnte er en del av DevOps.

Utfordringer med skyovervåking

En av de største utfordringene med skyovervåking for IT-team er å holde tritt med moderne og distribuerte applikasjonsdesign. Etter hvert som applikasjoner utvikler seg, må IT-teamene alltid justere overvåkingsstrategiene sine.

Effektiv skyovervåking er en kompleks oppgave. Verktøyene som en organisasjon bruker for øyeblikket, er kanskje ikke lenger de de trenger, da forskjellige typer applikasjoner må overvåkes på forskjellige måter.

Hvor er suksessen avhengig av?

Suksessen til enhver skyadministrasjonsstrategi avhenger ikke bare av riktig bruk av verktøy og automatisering, men også av å ha et kompetent IT-personale på plass. IT- og forretningsteam må samarbeide naturlig for å assimilere seg til en skykultur og forstå virksomhetens/organisasjonens mål.

IT-team må også teste ytelsen til skyprogrammer, overvåke databehandlingsmålinger i skyen, ta beslutninger om kritisk infrastruktur, løse oppdateringer og sikkerhetsproblemer og oppdatere forretningsreglene som driver skyadministrasjon.

Bedrifter / organisasjoner som mangler dyktige IT-ansatte kan alltid søke støtte fra tredjeparter. Tredjepartsapper støtter budsjett-terskelvarsler som kan varsle økonomi- og bransjeinteressenter, slik at de kan overvåke skyutgiftene sine. Skymeglinger har ofte en tjenestekatalog og noen økonomistyringsverktøy. Tiden for å granske skyutgifter er i starten, når apper går i produksjon.

Skyadministrasjonsplattformer, verktøy og leverandører

Etter hvert som databehandling i skyen utvides over hele bedriften, kan en generell plattform for skyadministrasjon hjelpe deg med å distribuere, administrere og overvåke alle skyressurser. Bedriftens IT må danne seg en klar idé om hva de vil overvåke før de evaluerer skyadministrasjonsplattformer for å passe disse behovene – enten det er individuelle verktøy som løser et enkelt problem, for eksempel nettverksytelse eller trafikkanalyse, eller en omfattende pakke som ser på alt. Noen av disse beslutningene vil veie verktøy fra skyleverandører, for eksempel sikkerhetsverktøy fra skyplattformleverandører eller fra tredjepartsleverandører.

De mest omfattende skyadministrasjonsproduktene tilbyr funksjoner som dekker disse fem kategoriene:

- automatisering og orkestrering for applikasjoner og individuelle virtuelle maskiner;
- sikkerhet, inkludert identitetsadministrasjon og databeskyttelse og kryptering;
- policystyring og overholdelse, inkludert revisjoner og servicenivåavtaler;
- ytelsesovervåking;
- kostnadsstyring.

Mange leverandører av multi-cloud-administrasjon tilbyr en rekke verktøy, hver med styrker og svakheter. Noen av de mer fremtredende er VMware (en virtualiserings- og cloud computing-programvareleverandør basert i Palo Alto, California. VMware ble grunnlagt i 1998 og er et datterselskap av Dell Technologies), CloudBolt Software (en hybrid skyadministrasjonsplattform utviklet av CloudBolt Software for distribusjon og administrasjon av virtuelle maskiner), applikasjoner og andre IT-ressurser, både i offentlige skyer (f.eks. AWS, MS Azure, GCP) og i private datasentre (f.eks. VMware, OpenStack)), Snow Software (som kjøpte Embotics, er en markedstestet utvikler av programvareforvaltningsverktøy), Morpheus Data (en ny tilnærming til å gi ekstern tilgang til mikrodata av offisiell statistikk), Scalr (en IT-leverandør som tilbyr en administrasjonsplattform for cloud computing) og Flexera (spesialiserer seg i IT-administrasjonsprogramvare, optimalisering og løsninger). Også i denne blandingen er tradisjonelle IT-service management leverandører, for eksempel BMC Software (baseboard management controller (BMC) er en spesialisert tjenesteprosessor som overvåker den fysiske tilstanden til en datamaskin, nettverksserver eller annen maskinvareenhet ved hjelp av sensorer og kommunikasjon med systemadministratoren gjennom en uavhengig tilkobling), CA Technologies (et av de største uavhengige programvareselskapene i verden. Selskapet, som tidligere var kjent som Computer Associates International, er et amerikansk multinasjonalt offentlig eid selskap), Micro Focus (en britisk multinasjonal programvare- og informasjonsteknologivirksomhet) og ServiceNow (en skybasert automatiseringsplattform for arbeidsflyt som gjør det mulig for bedriftsorganisasjoner å forbedre

driftseffektiviteten ved å effektivisere og automatisere rutinemessige arbeidsoppgaver), som vanligvis betjener store selskaper med ITSM-styringsprosesser (ITSM: Programvare for IT-tjenesteadministrasjon).

IT-bedrifter som bruker en enkelt offentlig sky, vil kanskje holde seg til verktøy som tilbys av den tjenesteleverandøren, fordi slike verktøy er utformet for å forbedre de opprinnelige administrasjonsplattformene. For skyovervåking overvåker Google Cloud Operations (tidligere Stackdriver) Google Cloud samt programmer og virtuelle maskiner som kjører på AWS Elastic Compute Cloud. Microsoft Azure Monitor samler inn og analyserer data og ressurser fra Azure-skyen. Det er også mange open source cloud monitoring alternativer for bedrifter som er komfortable med å jobbe med åpen kildekode-verktøy.

3 PROGRAMMER

3.1 Tilgang til en database ved hjelp av en persons fingeravtrykk som passord

Mål

Databaser inneholder noen ganger svært viktige data for enkelte selskaper eller organisasjoner. Tilgang til disse dataene er tillatt for et lite antall personer. For å øke sikkerhetsnivået må tilgangen til disse dataene baseres på bestemte indekser for de personene som har innsynsrett. Applikasjonen gir tilgang til databasen basert på fingeravtrykket til personene som har rett til å få tilgang til databasen.

Forventet tidsramme for å skape verdi

3 uker – 2 måneder

3.2 Active Directory-tjener

Mål

Målet med en Active Directory-server (AD) er å tilby en sentralisert plassering for administrasjon av nettverksressurser, for eksempel brukerkontoer, datamaskiner og skrivere. Det er et databaselager som lagrer informasjon om alle brukere og enheter som er koblet til et nettverk og lar autoriserte brukere få tilgang til ressurser på nettverket.

AD-serveren fungerer som en katalogtjeneste og er ansvarlig for å administrere godkjennings- og autorisasjonsprosessen for brukere som prøver å få tilgang til nettverksressurser. Dette gjør det mulig for systemansvarlige å håndheve sikkerhetspolicyer på tvers av organisasjonen, slik at bare autoriserte brukere

har tilgang til bestemte ressurser. AD-serveren tillater også delegering av administrative oppgaver til forskjellige enkeltpersoner eller grupper, noe som kan forbedre håndterbarheten og effektiviteten i en organisasjon. Samlet sett er det primære målet med en AD-server å forenkle nettverksadministrasjon, forbedre sikkerheten og gi et sentralisert administrasjonssted for alle nettverksressurser.

Forventet tidsramme for å skape verdi

Den forventede tidsrammen for å skape verdi med en Active Directory-server (AD) avhenger av organisasjonens spesifikke behov og krav. Noen fordeler kan imidlertid realiseres kort tid etter distribusjon, mens andre kan ta lengre tid å oppnå.

Når det gjelder umiddelbare fordeler, kan en AD-server forenkle nettverksadministrasjonen ved å sentralisere brukeradministrasjon. Dette kan forbedre effektiviteten og redusere tiden og innsatsen som kreves for vanlige IT-oppgaver, for eksempel tilbakestilling av passord eller oppretting av nye brukerkontoer. I tillegg kan AD i stor grad forbedre nettverkssikkerheten ved å tilby en sentralisert plassering for å håndheve sikkerhetspolicyer og administrere tilgang til nettverksressurser. Dette kan bidra til å redusere risikoen for sikkerhetsbrudd og uautorisert tilgang til bedriftsdata.

Andre fordeler, som forbedret skalerbarhet og fleksibilitet, kan ta lengre tid å realisere. AD-infrastrukturen kan for eksempel støtte organisasjonens vekst over tid ved å gi et skalerbart og pålitelig grunnlag for brukeradministrasjon og godkjenning. Dette kan bidra til å redusere kostnadene og øke effektiviteten etter hvert som organisasjonen utvides.

Samlet sett avhenger den forventede tidsrammen for å skape verdi med en AD-server av ulike faktorer, for eksempel organisasjonens størrelse og kompleksitet og de spesifikke tekniske kravene til distribusjonen. Noen fordeler kan realiseres umiddelbart, mens andre kan ta lengre tid å oppnå. Ikke desto mindre kan en AD-server være en verdifull investering når det gjelder å redusere administrative kostnader, øke sikkerheten og gi en skalerbar infrastruktur for organisasjonens langsiktige vekst.

3.3 AI-atferdsanalysesystemer

Mål

Målet med AI-atferdsanalysesystemer er å analysere og tolke menneskelige atferdsmønstre og forutsi fremtidig atferd basert på datadrevet innsikt. Den søker å gi en dypere forståelse av menneskelig atferd og beslutningstaking, og identifisere potensielle risikoer, trusler eller muligheter i ulike domener som politi, helsetjenester, sikkerhet og markedsføring. Ved å utnytte maskinlæringsalgoritmer og data mining-teknikker, tar disse systemene sikte på å identifisere mønstre og anomalier i atferd som kan indikere potensielle trusler

eller problemer. Det endelige målet er å utnytte innsikt fra atferdsanalyse for å forbedre beslutningstaking, redusere risiko og forbedre resultatene på mange felt.

Forventet tidsramme for å skape verdi

Tidsrammen for å skape verdi fra AI-atferdsanalysesystemer avhenger av flere faktorer, for eksempel kompleksiteten til problemet som løses, kvaliteten og tilgjengeligheten til data og teknologien som brukes.

I enklere scenarier kan verdier skapes relativt raskt, for eksempel i løpet av få måneder. For eksempel, hvis et selskap bruker atferdsanalysesystemer for å optimalisere sine markedsføringsstrategier, kan det se resultater på så lite som noen få måneder. På den annen side kan mer komplekse scenarier, for eksempel bruk av atferdsanalysesystemer for å oppdage svindel eller forhindre sikkerhetsbrudd, kreve mer forventet tidsramme for å skape verdi og kan ta flere år å realisere fullt ut.

Samlet sett kan et godt implementert AI-atferdsanalysesystem gi umiddelbare fordeler med forbedret beslutningstaking og risikoreduksjon, men det fulle potensialet til slike systemer kan ta lengre tid å materialisere seg. Etter hvert som algoritmene blir mer avanserte og datasettene blir mer omfattende, vil verdien skapt av disse systemene sannsynligvis fortsette å øke over tid.

3.4 Program for styring av utleie av verktøy og utstyr fra et selskap til fysiske personer

Mål

I mange situasjoner trenger personer som utfører reparasjonsaktiviteter i eget hjem spesifikke verktøy for disse aktivitetene. Noen reparasjons- eller konstruksjonsaktiviteter utføres sjelden, og det er ikke berettiget å kjøpe verktøy eller utstyr som er nødvendig for den aktiviteten.

En løsning er å leie dette utstyret fra selskaper som har dette aktivitetsobjektet. Søknaden styrer aktiviteten med å leie verktøy og utstyr til et selskap til personer eller andre selskaper som bruker dette utstyret.

Forventet tidsramme for å skape verdi

1 uke – 1 måned

3.5 Program for overvåking av autonomt rengjøringsutstyr (støvsugere) ved hovedkontoret til små og mellomstore bedrifter eller i private hjem

Mål

Applikasjonen tillater overvåking av aktiviteten til en robotstøvsuger eller flere robotstøvsugere som opererer autonomt i et lukket rom. Robotstøvsugere brukes til rengjøring av stuer eller kontorer.

Robotstøvsugere som kan betjenes med fjernkontroll og som kan bevege seg autonomt uten å bæres av en person, gjør rengjøring av et rom enklere.

Disse robotstøvsugerne er utstyrt med forskjellige typer sensorer som oppdager nærheten til et hinder og endrer støvsugerens bevegelsesretning. Robotstøvsugerens bevegelsesretning avhenger av måten robotstøvsugerens driftsalgoritme ble skrevet av produsenten.

Applikasjonen lager en algoritme for å flytte robotstøvsugeren i rommet slik at rengjøringsoperasjonen er effektiv.

Forventet tidsramme for å skape verdi

4 uker – 3 måneder

3.6 Sporing av aktiva

Mål

Målet med sporing av aktiva er å overvåke og administrere den fysiske plasseringen og tilstanden til eiendeler som utstyr, materialer og produkter når de beveger seg gjennom forsyningskjeden. Aktivasporingssystemer bruker avanserte teknologier som radiofrekvensidentifikasjon (RFID), globalt posisjoneringssystem (GPS) og strekkoding for å gi sanntidsinformasjon om plassering, status og bevegelser av eiendeler.

Noen av hovedmålene med sporing av aktiva inkluderer:

- Synlighet: Aktivasporingssystemer gir innsyn i plasseringen og statusen til eiendeler, slik at organisasjoner til enhver tid kan vite hvor eiendelene deres er.
- Samsvar: Sporingssystemer for aktiva hjelper organisasjoner med å overholde forskrifter ved å gi pålitelige data om bevegelse og håndtering av regulerte eiendeler som legemidler og farlige materialer.
- Effektivitet: Aktivasporingssystemer minimerer behovet for manuelle lagerkontroller og forbedrer effektiviteten i forsyningskjeden ved å gi sanntidsinformasjon om aktivabevegelser.

- Kostnadsreduksjon: Sporingssystemer for aktiva kan redusere kostnadene forbundet med tapte, stjålne eller feilplasserte eiendeler, og kan redusere tiden og arbeidet som kreves for å administrere lagerbeholdningen.
- Forbedret beslutningstaking: Aktivasporingssystemer gir data som kan brukes til å støtte bedre beslutningstaking, for eksempel optimalisering av forsyningskjedeoperasjoner, prognoser for fremtidig etterspørsel og identifisering av ineffektivitet.

Samlet sett er målet med aktivasporing å gi organisasjoner sanntidsdataene de trenger for å effektivt administrere eiendelene sine, forbedre ytelsen i forsyningskjeden, redusere kostnadene og ta informerte beslutninger om driften. Ved å utnytte denne innsikten kan organisasjoner forbedre driften, forbedre kundeopplevelsen og få et konkurransefortrinn i bransjen.

Forventet tidsramme for å skape verdi

Den forventede tidsrammen for å skape verdi fra løsninger for aktivasporing vil avhenge av organisasjonens spesifikke behov og kompleksiteten til løsningen for aktivasporing som distribueres. I mange tilfeller kan imidlertid organisasjoner forvente å se fordelene med sporing av aktiva innen noen måneder til ett år etter implementering.

På kort sikt kan sporing av eiendeler gi umiddelbare fordeler som å redusere risikoen for tapte eller stjålne eiendeler, forbedre lagernøyaktigheten og optimalisere ressursutnyttelsen. Disse fordelene kan oppnås relativt raskt, ofte innen få uker eller måneder etter implementering.

På lengre sikt kan verdien som skapes av sporing av aktiva øke etter hvert som organisasjonen får bedre innsyn i forsyningskjedeoperasjonene og identifiserer muligheter for optimalisering og forbedring. Dette kan føre til ytterligere kostnadsbesparelser, høyere kundetilfredshet og forbedret effektivitet.

Etter hvert som teknologien fortsetter å utvikle seg og løsninger for sporing av aktiva blir mer avanserte, vil potensialet for verdiskaping fortsette å vokse. Maskinlæring og prediktiv analyse kan for eksempel brukes til å identifisere mønstre og trender i aktivabevegelser, slik at organisasjoner kan forutse forstyrrelser i forsyningskjeden og iverksette forebyggende tiltak.

Samlet sett vil den forventede tidsrammen for å skape verdi fra løsninger for aktivasporing variere avhengig av organisasjonens spesifikke behov. Ved å implementere en løsning for aktivasporing kan organisasjoner imidlertid forvente å se en positiv innvirkning på driften, effektiviteten og bunnlinjen innen en relativt kort tidsramme.

3.7 Oppmøtesporing for studenter

Mål

Oppmøtesystem er et system som brukes til å spore tilstedeværelsen til en bestemt person og brukes i industrien, skoler, universiteter eller arbeidsplasser. Den tradisjonelle måten å ta oppmøte på har ulempe, som er at dataene i oppmøtelisten ikke kan gjenbrukes og sporing og sporing av studentens oppmøte er vanskeligere. Det teknologibaserte oppmøtesystemet som sensorer og biometribasert oppmøtesystem reduserte menneskelig involvering og feil. I denne artikkelen presenteres derfor et NFC-basert oppmøtesystem. En komparativ studie mellom dette både NFC og RFID diskuteres også grundig, spesielt når det gjelder arkitekturer, funksjonalitetsfunksjoner, fordeler og svakhet. Totalt sett øker til og med både NFC- og RFID-oppmøtesystemet effektiviteten ved opptak av oppmøte, NFC-systemet gir flere bekvemmeligheter og billigere infrastruktur i både drifts- og installasjonskostnader.

Forventet tidsramme for å skape verdi

3 – 6 måneder

3.8 Automatisert anleggsadministrasjon

Mål

Målet med automatisert anleggsadministrasjon er å bruke teknologi til å strømlinjeforme og automatisere bygnings- og anleggsadministrasjonsprosesser for å forbedre driftseffektiviteten, redusere kostnadene og forbedre beboeropplevelsen. Dette inkluderer bruk av smarte bygningsteknologier som muliggjør overvåking, kontroll og optimalisering av ulike bygningssystemer, inkludert VVS, belysning, sikkerhet og energiforbruk.

Noen av hovedmålene for automatisert anleggsadministrasjon inkluderer:

- Forbedret driftseffektivitet: Ved å automatisere prosesseen for anleggsadministrasjon kan organisasjoner redusere tiden og ressursene som trengs for å administrere anleggene sine, slik at de kan fokusere mer på kjernevirksomhet.
- Reduserte kostnader: Automatisert anleggsadministrasjon kan hjelpe organisasjoner med å redusere energiforbruket, minimere vedlikeholdskostnadene og optimalisere ressursallokeringen.
- Forbedret bygningsytelse: Ved å utnytte dataanalyse og sanntidsovervåking kan automatiserte anleggsstyringssystemer oppdage og løse problemer med bygningens ytelse raskere, noe som resulterer i bedre bygningsytelse og lavere driftskostnader.

- Forbedret beboeropplevelse: Automatisert anleggsadministrasjon kan forbedre beboeropplevelsen ved å tilby mer komfortable og sikre miljøer gjennom sanntidsovervåking og optimalisering av ulike bygningssystemer.
- Samsvar: Ved å automatisere og standardisere prosesser kan automatisert anleggsadministrasjon hjelpe organisasjoner med å overholde forskrifter og retningslinjer, og redusere risikoen for bøter, straffer og rettssaker.

Samlet sett er målet med automatisert anleggsadministrasjon å utnytte teknologi for å gjøre det mulig for organisasjoner å oppnå bedre overordnet styring av sine bygninger og anlegg. Ved å øke effektiviteten, redusere kostnadene og forbedre beboeropplevelsen, kan organisasjoner bli mer konkurransedyktige og betjene kundene sine bedre.

Forventet tidsramme for å skape verdi

Den forventede tidsrammen for å skape verdi fra automatisert anleggsadministrasjon vil avhenge av flere faktorer, for eksempel størrelsen og kompleksiteten til bygningen eller anlegget, typen teknologi som brukes, og de spesifikke målene for organisasjonen.

I mange tilfeller kan organisasjoner forvente å se målbare fordeler fra sine automatiserte fasilitetsstyringssystemer innen noen måneder til et år etter implementering. Disse fordelene kan omfatte:

- Redusert energiforbruk: Automatisert anleggsadministrasjon kan optimalisere ulike bygningssystemer, redusere energiforbruket og resultere i lavere energiregninger.
- Strømlinjeformede vedlikeholdsprosesser: Ved å automatisere vedlikeholdsprosesser kan organisasjoner redusere behovet for manuell inngripen, spare tid og redusere kostnadene.
- Forbedret beboeropplevelse: Automatisert anleggsadministrasjon kan forbedre bygningens komfortnivå, noe som resulterer i økt beboertilfredshet.
- Bedre driftseffektivitet: Automatisert anleggsadministrasjon kan strømlinjeforme ulike bygningsadministrasjonsprosesser, noe som resulterer i forbedret effektivitet og reduserte organisasjonskostnader.
- Prediktivt vedlikehold: Ved å ta i bruk prediktivt vedlikehold kan organisasjoner forbedre levetiden til bygningssystemene og redusere reparasjonskostnadene.

Samlet sett vil den forventede tidsrammen for å skape verdi fra automatisert anleggsadministrasjon avhenge av organisasjonens spesifikke behov og kompleksiteten til systemene som implementeres. Men ved å utnytte fordelene.

3.9 Automatisering av oppgaver ved hjelp av skybaserte tjenester: anbefalingsmotor

Mål

Market Basket Analysis er en modelleringsteknikk basert på teorien om at hvis du kjøper en bestemt gruppe varer, er det mer (eller mindre) sannsynlig at du kjøper en annen gruppe varer. I detaljhandel kjøpes de fleste kjøp på impuls. Markedskurvanalyse gir informasjon om hva en kunde kunne ha kjøpt hvis ideen hadde kommet opp for dem.

Forventet tidsramme for å skape verdi

1 – 6 måneder

3.10 Back-Up / Katastrofehjelp

Mål

Å ha et automatisk system for sikkerhetskopiering av kritiske data på tvers av flere forskjellige regioner for å minimere risikoen for katastrofale feil, slik at hvis det er en feil i en hel region, vil sikkerhetskopiene være upåvirket, i motsetning til å ha sikkerhetskopier satt opp på forskjellige servere i samme region, hvor en total regionfeil vil føre til tap av data selv med sikkerhetskopier.

Forventet tidsramme for å skape verdi

N/A

3.11 Chatbot for å indikere ledige plasser på offentlige parkeringsplasser i en by

Mål

Et problem som alle bilførere står overfor er behovet for å finne ledige plasser på offentlige parkeringsplasser i byen, så nært som mulig det stedet de ønsker å dra til. Dette er ganske vanskelig fordi sjåføren er i trafikken og må orientere seg i henhold til situasjonen i området.

En løsning som løser problemet og letter sjåførens oppgave er en chatbot-type applikasjon på sjåførens mobiltelefon. Føreren kommuniserer med applikasjonen med stemmen og finner ut på forhånd situasjonen med gratis parkeringsplasser på parkeringsplassene som ligger i nærheten av området der sjåføren har

problemer å løse.

Forventet tidsramme for å skape verdi

1 måned og en halv – 10 måneder

3.12 Chatbot for å tilpasse læringsaktiviteten til elever i yrkesfaglig videregående opplæring

Mål

Tradisjonelt sett lærer elevene ved å lese leksjonen skrevet på papir eller ved å lese leksjonen skrevet i elektronisk format i en word-fil eller lignende formater (pdf, etc.). Leksjonen blir vanligvis fulgt av et sett med spørsmål der studenten kan sjekke hvordan han lærte leksjonen

Applikasjonen som er foreslått nå, hjelper studenten til å lære på en interaktiv måte med mer effektivitet.

Forventet tidsramme for å skape verdi

1 måned – 6 måneder

3.13 Chatbot for studenter i EDU-institusjon

Mål

Mange programvareselskaper prøver å bygge minst en enkel FAQ / Q&A basert chatbot. Nylige arbeider viser at det er veldig enkelt å bygge en bot, mens å bygge en intelligent en kan være ekstremt vanskelig (og dyrt). Domenespesifikke roboter som AI-drevne Support Center Automation Bots bør vurdere å være interoperable på mange nivåer, og med hvert nytt nivå vokser kompleksitetsnivået eksponentielt. De siste årene har meldingsapper har gått forbi sosiale nettverk og blitt de dominerende plattformene på smarttelefoner. Det enorme potensialet bør vurderes for å løse et av problemene som enhver organisasjon større enn 10 deltakere har. Ved å kombinere ulike eksisterende og eksterne datakilder som selskapet allerede har tilgang til, kunne de fleste av første- og andrelinje-helpdesk-spørsmålene løses før de kom til supportpersonalet. Robotic Process Automation (RPA) er et av de heteste temaene blant eksperter på forretningsprosesser, mens et av de raskest voksende feltene innen RPA er kunnskapsutvinning, som er spesielt aktuelt i utdanningsmiljø (EDU) som alle typer EDU-støttesystemer.

Forventet tidsramme for å skape verdi

3 – 9 måneder

3.14 Skybasert e-læring

Mål

Den økende forskningen innen informasjonsteknologi har en positiv innvirkning på utdanningsverdenen. Implementeringen av e-læring er et bidrag fra informasjonsteknologi til utdanningsverdenen. Implementeringen av e-læring er implementert av flere utdanningsinstitusjoner i Indonesia. E-læring gir mange fordeler som fleksibilitet, mangfold, måling og så videre. De nåværende e-læringsapplikasjonene krevde store investeringer i infrastruktursystemer, uavhengig av kommersiell eller åpen kildekode e-læringsapplikasjon. Hvis institusjonen hadde en tendens til å bruke åpen kildekode-e-læringsapplikasjon, ville det kreve mer kostnad å ansette profesjonelt personale for å vedlikeholde og oppgradere e-læringsapplikasjonen. Det kan være utfordrende å implementere e-læring i utdanningsinstitusjonene. Et annet problem som kan oppstå i bruken av e-læringstrenden i dag, er mer sannsynlig at institusjonen bygger sitt eget e-læringssystem selv. Hvis to eller flere institusjoner er villige til å bygge og bruke en e-læring slik at de kan minimere utgiftene til å utvikle systemet og dele læringsmateriell, har det sannsynligvis skjedd. Denne rapporten diskuterer dagens tilstand og utfordringer i e-læring og forklarte deretter det grunnleggende konseptet og tidligere foreslåtte arkitekturer for cloud computing. I denne artikkelen foreslo forfatterne også en modell for skybasert e-læring som består av fem lag, nemlig: (1) infrastrukturlag; (2) plattformlag; (3) applikasjonslag; (4) tilgangslag; og (5) brukerlag. I tillegg til denne artikkelen illustrerte vi også skifteparadigmet fra konvensjonell e-læring til skybasert e-læring og beskrev de forventede fordelene ved å bruke skybasert e-læring.

Forventet tidsramme for å skape verdi

6 – 12 måneder

3.15 Kommunikasjon / Informasjonsutveksling Applikasjon/ Kanaler

Mål

Målet med kommunikasjons-/informasjonsutvekslingsapplikasjoner er å muliggjøre sømløs og effektiv kommunikasjon og deling av informasjon mellom enkeltpersoner eller grupper. Disse applikasjonene gir brukerne en plattform for å få kontakt med andre, samarbeide og få tilgang til informasjon i sanntid, uavhengig av hvor de befinner seg.

Med kommunikasjons-/informasjonsutvekslingsprogrammer kan brukere dele dokumenter, filer og andre former for data, gjennomføre lyd- og videokonferanser, direktemeldinger og dele skjermer. Det endelige målet er å forbedre produktiviteten, forbedre samarbeidet og strømlinjeforme arbeidsflyter.

I tillegg gir disse programmene ofte sikkerhetsfunksjoner som ende-til-ende-kryptering for å beskytte sensitiv informasjon. Noen kommunikasjons-/informasjonsutvekslingsprogrammer inkluderer også AI-drevne funksjoner som dokumentoversettelse, sentimentanalyse og automatisk transkripsjon for å gjøre kommunikasjonen mer effektiv og effektiv.

Samlet sett er målet med kommunikasjons- / informasjonsutvekslingsapplikasjoner å legge til rette for effektiv kommunikasjon og samarbeid, noe som fører til forbedret ytelse, forbedret kundetilfredshet og økt lønnsomhet for bedrifter og organisasjoner.

Forventet tidsramme for å skape verdi

Den forventede tidsrammen for å skape verdi for en kommunikasjons-/informasjonsutvekslingsapplikasjon kan variere basert på flere faktorer, inkludert applikasjonens kompleksitet, omfang og teknologistakken som brukes til å utvikle den.

For mindre applikasjoner med begrensede funksjoner kan verdien opprettes i løpet av få uker eller måneder. Slike applikasjoner kan være en enkel meldings- eller fildelingsplattform som tar sikte på å koble eksterne arbeidere eller lagkamerater.

For større programmer med komplekse funksjoner som gruppevideosamtaler, interaktive tavler, dokumentsamarbeid og andre avanserte funksjoner, kan det ta flere måneder eller til og med år å skape verdi.

Utviklingstiden vil også avhenge av teamets ressurser, erfaring og metodikken som brukes til å bygge applikasjonen. Den smidige metodikken som involverer iterativ utvikling og regelmessig tilbakemelding fra brukere, kan bidra til å forkorte utviklingssyklusen og raskt skape verdi.

Samlet sett kan en kommunikasjons-/informasjonsutvekslingsapplikasjon skape verdi så snart den blir operativ og begynner å legge til rette for effektivt samarbeid og forbedre produktiviteten for brukerne. Nøkkelen er å fokusere på å lage et program som oppfyller brukernes behov, er enkel å bruke, og gir en tilfredsstillende opplevelse som vil holde dem ved hjelp av programmet på lang sikt.

3.16 Kontinuerlig overvåking av driften av noen industrielle installasjoner ved hjelp av cloud computing og IoT-teknologier

Mål

De industrielle installasjonene som tilhører noen selskaper, kan utgjøre en fare dersom verdiene til noen parametere som karakteriserer disse installasjonene er utenfor området for normal drift.

Et eksempel er tanklagringen som inneholder den flytende propan-butanblandingen som brukes til å drive væsken inne i sprøytebeholderne.

Denne gassen tappes på flaske i mindre beholdere sammen med væsken som skal sprayes ved å trykke på en knapp. Applikasjonen overvåker visse mengder (gasstrykk, tanktemperatur, etc.) av installasjonen.

Når de overvåkede parametrene nærmer seg farlige verdier, blir det truffet tiltak for å bringe driften av installasjonen til normale parametere.

Forventet tidsramme for å skape verdi

3 uker 4 måneder

3.17 Kontinuerlig pasientovervåking

Mål

Et system som bruker sensorer sammen med IoT-huben som kan fjernovervåke pasientens vitalitet og heve advarsler hvis visse nivåer går utenfor visse terskler

Forventet tidsramme for å skape verdi

1 år – 1,5 år

3.18 Opprette testmiljøer

Mål

Klargjør og opprett ressursene som trengs for å kjøre testversjoner av eksisterende distribusjoner, slik at nye funksjoner eller mulige feilrettinger kan skrives og kjøres uten å forstyrre gjeldende distribusjon som kjører.

Forventet tidsramme for å skape verdi

1 uke

3.19 Opprette en didaktisk applikasjon for å hjelpe elevene å lære et fremmedspråk

Mål

Applikasjonen er utviklet for pedagogiske formål. Den er designet for å lette å lære et fremmedspråk. Det er fremmedspråk der for hver lyd (fonem) som utgjør et ord når det uttales, brukes det samme grafiske elementet (grafem) til å registrere det uttalte ordet skriftlig. På andre språk, for samme lyd, brukes to eller tre kombinasjoner av grafiske elementer for å fikse ordet skriftlig.

For å lette læringen av et fremmedspråk ble det internasjonale fonemiske alfabetet introdusert, som alltid bruker det samme grafiske symbolet for å registrere den samme talte lyden skriftlig. Dette gjør det lettere å lære et fremmedspråk.

Ved å bruke applikasjonen kan studenten lære riktig uttale av ordene på fremmedspråket som skal læres.

Forventet tidsramme for å skape verdi

3 uker – 3 måneder

3.20 Sikkerhetskopiering og arkivering av data

Mål

Sikkerhetskopi. Arkiv. Datalagringsmetode. De opprinnelige dataene forblir på plass, mens en sikkerhetskopi lagres på et annet sted. Arkiverte data flyttes fra den opprinnelige plasseringen til et arkivlager.

Å leve i en verden der nettkriminalitet er dagens orden. Det vil ikke gå en dag uten tilfeller av store datainnbrudd, som til tider blir fatale for ganske mange virksomheter.

Tradisjonelle metoder for sikkerhetskopiering av data har vist seg å være effektive for sikkerhetskopiering av data i lang tid. Ikke desto mindre er de utsatt for virus, og på grunn av deres bærbare natur kan de gå seg vill og utgjøre en trussel mot moderne virksomheter.

Skybasert sikkerhetskopiering og arkivering er en løsning på disse utfordringene. Det er enkelt å implementere og gir maksimal datasikkerhet. Med denne tilnærmingen kan du sikkerhetskopiere eller arkivere sensitive filer til skybaserte lagringssystemer. Dette gir forsikring om at dataene dine fortsatt er intakte selv om live-dataene dine på en eller annen måte blir kompromittert.

Noen skydatabehandlingstjenester lar deg planlegge sikkerhetskopiering for å dekke dine unike behov. I tillegg kan du kryptere skysikkerhetskopiene dine og gjøre det umulig for hackere og snushaner å få tilgang.

Med skylagring kan du få så mye plass du trenger og lagre så mye data du trenger, og betaler bare for det du faktisk bruker.

Forventet tidsramme for å skape verdi

Tidsrammen for verdiskaping kan variere avhengig av organisasjonens spesifikke behov og nivået på implementering av sikkerhetskopiering og arkivering, men fordelene kan begynne å påløpe fra den aller første implementeringen.

3.21 Hindring av tap av data skybasert system

Mål

DLP (Data Loss Prevention) er et sikkerhetsverktøy for databeskyttelse, og dets kompleksitet og teknologiske utvikling bidrar til en svært liten forståelse av funksjonaliteten og egenskapene til verktøyet. Med forskjellige navn og teknologiske tilnærminger kan det være vanskelig å forstå den endelige verdien av verktøyet og det som passer best til miljøene. Det er en mangfoldig forståelse av hva DLP-løsningen er. Noen anser det for å kryptere eller kontrollere USB-inngangen til DLP, mens andre ser bredere ut.

DLP er definert som: produkter som, basert på sentrale retningslinjer, identifiserer, overvåker og beskytter søvn-, bevegelses- og bruksdata gjennom dyp innholdsanalyse. Viktige DLP-funksjoner er:

1. Analyse av innhold

2. Sentral politikkstyring

3. Dekk innhold på flere plattformer og steder

DLP-løsninger beskytter sensitive data og hjelper organisasjoner med å forstå dataene sine bedre og forbedre deres evne til å administrere innhold.

Forventet tidsramme for å skape verdi

6 – 12 måneder

3.22 Datahåndteringssystem om selskapets ansatte

Mål

Generelt administrerer små bedrifter med et lite antall ansatte ansattdata ved hjelp av Excel- eller Word-filer der de lager tabeller. Dataene til de ansatte er skrevet i disse tabellene. Disse tabellene har ikke et enhetlig format, og endring av noen data om ansatte krever noen ganger endringer i flere filer.

Når endringer gjøres, er det mulig at noen filer ikke endres, og i andre filer kan viktige data om ansatte bli ødelagt ved et uhell. I tillegg krever tilgang til informasjon om en ansatt visning av alle Excel- eller Word-dokumenter.

Den foreslåtte applikasjonen gir mulighet til å lagre ansattdata i en relasjonsdatabase lagret enten på ens egen server eller på et annet selskaps server. I tillegg er det grafiske grensesnittet som brukes vennlig og suggestivt.

Forventet tidsramme for å skape verdi

2 uker - 2 måneder

3.23 Sertifisering av digitale eiendeler ved bruk av distribuert hovedbok/blokkjede

Mål

Hovedtrekkene i blockchain er åpenhet og desentralisering, som dagens systemer ikke kan skryte av. Digital identitet kombinert med blockchain-teknologi vil gjøre det mulig for folk å utføre oppgaver som er raskere, enklere og sikrere, inkludert bevis på identitet, fakta, status og data. Utrolig nok er faktum at det å søke etter nye ansatte, sjekke kandidatdata og selve jobbsøknaden kan være en prosess som bare vil ta et par museklikk på datamaskinen, med stor sikkerhet for at dataene blir oppnådd. Men blockchain tilbyr det bare. Ved å plassere all informasjon om vår identitet på den, med kryptografi som gjør det hele trygt og gjennomsiktig og alltid tilgjengelig via internett, bruker vi all tid brukt på å bevise identitet, data, fakta og tilstand på de viktigste tingene. Tenk deg at vi også kan legge ved 3 kryptografiske nøkler sammen med søknaden om virksomhet, slik at arbeidsgiver enkelt kan sjekke med absolutt sikkerhet at vi faktisk har fullført den høyskolen vi har oppgitt i CV-en hans, om vi mistrives og om vi i det hele tatt er en person som utgir seg for å være det. Denne prosessen vil ta omtrent noen minutter, mens den samme prosessen varer i flere dager, om ikke uker, ettersom dataverifiseringen gjøres ved å skrive spørringer i hvert av disse systemene som data kommer fra.

Forventet tidsramme for å skape verdi

3 – 9 måneder

3.24 Digital identitet

Mål

Identitet er veldig verdifullt for oss, og ikke for institusjoner, vi oppfører oss ikke deretter. På grunn av mangel på bevissthet og utdanning om identitet i seg selv, på grunn av den digitale og fysiske sentraliseringen av databaser og data om våre identiteter, noe som skaper uunngåelige svakheter som undergraver den systematiske verdien av våre personopplysninger. Sentraliserte systemer er en god bytte for angripere med dårlige intensjoner fordi hvis de bryter seg inn i systemet, kan de enkelt stjele (kopiere) store mengder data som er lagret i det systemet. Vi har vært vitne til mange angrep på sentraliserte systemer, ikke små forretningssystemer, men store og globalt innflytelsesrike selskaper som Yahoo, eBay, Adobe, JP Morgan, Chase, Sony og mange andre.

Blockchain-teknologi tilbyr løsningen på dette problemet som blir mer og mer konstant på grunn av konstante behov, økt etterspørsel og bruk av digital identitet. Men som vi nevnte tidligere, er dette en ny teknologi og er bare i de tidlige stadiene av prosjektet, og vi undersøker fortsatt alle mulighetene og anvendelsen av denne teknologien. Med behovet for å bevise vår identitet, møtes vi hver dag og på forskjellige steder. På jobb, i bank, i butikk, på reise, i statlige institusjoner og på mange forskjellige steder. For tiden er det mange nye og potensielle prosjekter og unge selskaper som arbeider med dette problemet og prøver å finne sin plass i markedet. I denne delen vil vi nevne noen av dem og mer spesifikt forklare deres forretningsmodeller.

Forventet tidsramme for å skape verdi

1 – 3 måneder

3.25 Digital twinning

Mål

Opprett et virtuelt miljø basert på et virkelig system, ved hjelp av sensorer og IoT-evner, og utforsk muligheter og konsekvenser av å endre miljøet, overvåke tilstanden til systemer slik at vedlikehold og reparasjoner kan gjøres etter hvert som behovet oppstår, i stedet for å ha planlagte inspeksjoner.

Ved å observere dataene som samles inn fra sensorene, kan du simulere endringer i miljøet for å se hvordan systemet vil reagere og få innsikt i hvordan du kan forbedre ytelsen til systemet. For eksempel kan det brukes til å forbedre ytelsen for et ventilasjonssystem ved mer dynamisk bruk der det øker arbeidsflyten i travle tider og områder og sparer energi når det er mindre behov, noe som skaper både et mer behagelig miljø og reduserer energikostnadene.

Forventet tidsramme for å skape verdi

6 måneder – 1 år

3.26 Plattform for katastrofeforebygging

Mål

Ved hjelp av Internett-aktiverte miljøsensorenheter som sender data til en skybasert analyseserver som genererer alarm og rapporter basert på analyse av dataene.

En omfattende overvåkingsløsning for innsamling, analyse og respons på telemetri fra skyen og lokale miljøer. Maksimere tilgjengeligheten og ytelsen til programmene og tjenestene dine.

Innsamling og integrering av data fra hvert lag og hver komponent i systemet ditt i en felles dataplattform. Den korrelerer data på tvers av flere abonnementer og leiere, i tillegg til å være vert for data for andre tjenester. Fordi disse dataene er lagret sammen, kan de korreleres og analyseres ved hjelp av et felles sett med verktøy. Dataene kan deretter brukes til analyse og visualiseringer for å hjelpe deg med å forstå hvordan programmene yter og reagere automatisk på systemhendelser.

Forventet tidsramme for å skape verdi

Tidsrammen for å skape verdi for en slik plattform vil avhenge av ulike faktorer som plattformens kompleksitet, tilgjengelige ressurser og kompetansenivået til teamet som utvikler plattformen. I noen tilfeller kan verdien av en plattform for katastrofeforebygging være umiddelbart tydelig, mens det i andre tilfeller kan ta litt tid å analysere og måle effektiviteten. Til syvende og sist vil suksessen og verdien av en katastrofeforebyggingsplattform avhenge av dens evne til å forhindre eller redusere virkningen av katastrofer.

3.27 Distribusjon av pakker i en geografisk region ved hjelp av autonome droner

Mål

For noen århundrer siden ble trente duer (også kalt vandreduer) brukt til å overføre meldinger mellom avsender og mottaker. Det er i hvert fall det historiene som har nådd oss sier.

Det var fordeler og ulemper med denne måten å overføre meldinger på. En måte å overføre pakker mellom et distribusjonspunkt og ulike mottakere kan være å bruke autonome droner.

Forventet tidsramme for å skape verdi

3 uker – 6 måneder

3.28 Deteksjon av dokumentlikhet og system for uttrekking av dokumentinformasjon

Mål

Det er en menneskelig tendens til å formulere antagelser mens man analyserer vanskeligheten med informasjonsutvinning i dokumenter. Vi antar automatisk at det er enklere å trekke ut informasjon i form av navngitte enheter fra et sett med lignende dokumenter. Ikke desto mindre har lignende dokumenter et distinkt sett med problemer. De navngitte enhetene i disse dokumenttypene varierer i størrelse, i likhet med antall tegn, ord, høyde, bredde og plassering. Disse variasjonene kan ikke håndteres ved hjelp av heuristikk eller forhåndstrente språkmodeller.

Forventet tidsramme for å skape verdi

6 – 12 måneder

3.29 Oversettelse av dokumenter

Mål

Oversette dokumenter som inneholder beskrivelser av produktene som selges på et nettsted, slik at virksomheten kan imøtekomme en bredere demografisk og kan resultere i økte salgstall. Å sørge for at et nettsted er tilgjengelig på forskjellige språk er spesielt viktig når du prøver å appellere til et internasjonalt publikum, eller virksomheten leverer et område eller en bransje som består av mange ikke-majoritetshøyttalere.

Når man er i et flerspråklig rom kan det også være nyttig å automatisk oversette brukergenerert innhold, for eksempel produktanmeldelser, eller å opprette og vedlikeholde en database med vanlige spørsmål på flere forskjellige språk.

Forventet tidsramme for å skape verdi

3 måneder – 6 måneder

3.30 Dynamisk webhotell

Mål

Et webvertsmiljø inneholder detaljer som er spesifikke for applikasjonen, for eksempel hvor applikasjonen er lagret på og funksjoner og tjenester som er avgjørende for å administrere hele applikasjonen. De vanligste typene webhotell er: statisk hosting, dynamisk hosting og lokal hosting.

Forventet tidsramme for å skape verdi

1 – 3 måneder

3.31 Dynamisk nettside med datalagring i en database

Mål

Hjemmesider er svært populære i disse dager og tillater informasjon som skal vises på en attraktiv og vennlig måte. Informasjonen på disse nettstedene er i form av tekst eller bilder. Noen nettsteder kan ha mange sider, avhengig av formålet. Ofte må informasjonen de overfører endres relativt ofte på grunn av visse forhold.

For eksempel endrer en pizzeria som har en nettside menyen daglig. Nettsiden må oppdateres daglig. I dette tilfellet må eieren av pizzeriaen (jeg valgte en pizzeria som eksempel, men det kan være andre eksempler) kontakte personen som laget nettstedet daglig for å oppdatere informasjonen. Et dynamisk nettsted som viser informasjon ved hjelp av en database, er velkommen.

Forventet tidsramme for å skape verdi

2 uker - 1 måned

3.32 E-handel applikasjon

Mål

Hovedmålet med en e-handelsapplikasjon er å muliggjøre elektroniske kommersielle transaksjoner mellom bedrifter og forbrukere over internett. E-handelsapplikasjoner gjør det mulig for bedrifter å selge sine produkter og tjenester på nettet, og forbrukere å kjøpe disse produktene og tjenestene over internett.

Målet med en e-handelsapplikasjon er å gi forbrukerne en sømløs handleopplevelse, samtidig som det gir bedrifter en kostnadseffektiv måte å selge sine produkter og tjenester på. Applikasjonen skal være utformet for å være intuitiv, enkel å bruke og gi praktiske betalingsalternativer, slik at kundene enkelt kan handle.

I tillegg bør en e-handelsapplikasjon utformes for å gi bedrifter robuste rapporterings- og analysefunksjoner, slik at de kan spore salgsdata, lagernivåer, kundekjøpsmønstre og andre viktige beregninger. Dette hjelper bedrifter med å identifisere trender og ta datadrevne beslutninger som fremmer forretningsvekst og suksess.

Samlet sett er målet med en e-handelsapplikasjon å legge til rette for sikker og praktisk online kjøp, samtidig som det gjør det enkelt for bedrifter å administrere sine online transaksjoner. Ved å gi kundene en strømlinjeformet, brukervennlig handleopplevelse og bedrifter effektive styringsverktøy, kan en e-handelsapplikasjon øke salg, inntekter og markedsandeler for bedrifter betydelig.

Forventet tidsramme for å skape verdi

Tidsrammen for å skape verdi fra en e-handelsapplikasjon avhenger av flere faktorer, inkludert størrelsen og kompleksiteten til programmet, nivået av tilpasning som kreves, og ressursene som er tilgjengelige for utvikling.

Vanligvis kan det ta flere måneder til et år å designe, utvikle, teste og lansere en e-handelsapplikasjon. Bedrifter kan imidlertid begynne å generere verdi fra en e-handelsapplikasjon selv før den er fullført hvis de følger en smidig utviklingstilnærming, noe som gjør dem i stand til å levere små verdiøkninger til kundene raskere.

I de tidlige stadiene av applikasjonsutvikling for e-handel, bør bedrifter fokusere på å skape et minimum levedyktig produkt (MVP) som gir et grunnleggende sett med funksjoner og funksjonalitet for kunder å handle online. Dette gjør det mulig for bedrifter å validere antagelsene sine og teste markedet før de investerer mer ressurser i å utvikle tilleggsfunksjoner.

Når MVP er lansert, kan bedrifter begynne å generere verdi ved å måle viktige ytelsesberegninger som nettstedstrafikk, konverteringsfrekvenser og kundetilfredshetsnivåer. De kan bruke disse dataene til å gjenta og forbedre programmet kontinuerlig, og legge til nye funksjoner og funksjonalitet for å drive kundeengasjement, salg og inntekter.

Samlet sett, mens den forventede tidsrammen for å skape verdi fra en e-handelsapplikasjon kan avhenge av ulike faktorer, kan bedrifter begynne å realisere fordelene fra de tidlige utviklingsstadiene og kontinuerlig forbedre og forbedre funksjonene over tid for å drive kundeengasjement og vekst.

3.33 Elektronisk katalog med elevenes skoleresultater

Mål

Søknaden registrerer i en database resultatene oppnådd av videregående studenter i fagene som studeres på skolen. Applikasjonen analyserer resultatene til hver enkelt elev, og når resultatene er under beståttgrensen eller er nær grensen, varsler den dette ved å sende en e-post eller en advarsel på mobiltelefonen til foreldrene.

Forventet tidsramme for å skape verdi

1 uke - 1 og en halv time

3.34 Adgangskontroll for fasiliteter

Mål

Målet med Facilities Access Control er å sikre at bare autoriserte personer har tilgang til et bestemt fysisk sted eller anlegg. Adgangskontroll bidrar til å forhindre uautorisert tilgang, tyveri og hærverk, og kan også bidra til å opprettholde de ansattes sikkerhet og sikkerhet. Ved å implementere tilgangskontrolltiltak kan en organisasjon beskytte sensitive områder av anlegget mot uautorisert oppføring, beskytte eiendeler og informasjon, og redusere risikoen for skade på ansatte.

Facility Access Control innebærer vanligvis å bruke et elektronisk system som vil kreve autoriserte personer til å presentere legitimasjon eller identifikasjon for å få tilgang til begrensede områder. Systemet kontrollerer legitimasjonen som presenteres mot en database med autoriserte personer, og gir bare tilgang hvis den presenterte legitimasjonen samsvarer med en autorisert oppføring i databasen. Elektroniske adgangskontrollsystemer kan konfigureres til å gi tilgang til ulike sikkerhetsnivåer. For eksempel kan ansatte få tilgang til områder som er relevante for arbeidet deres, mens svært sensitive områder kan kreve ytterligere sikkerhetstiltak, for eksempel biometriske data eller dobbel autentisering.

Samlet sett er målet med tilgangskontroll for fasiliteter å gi et sikkert miljø for enkeltpersoner og eiendeler i en organisasjon. Adgangskontrolltiltak kan bidra til å redusere risikoen for skade, tyveri og uautorisert oppføring, samt forbedre ansattes tillit og sikkerhet.

Forventet tidsramme for å skape verdi

Den forventede tidsrammen for å skape verdi med Facilities Access Control avhenger av den spesifikke implementeringen og kravene til organisasjonen. Noen fordeler med tilgangskontroll kan imidlertid oppleves umiddelbart, mens andre kan ta lengre tid å realisere.

Umiddelbare fordeler kan inkludere forbedret sikkerhet og redusert risiko for tyveri, hærverk eller uautorisert tilgang. Dette kan bidra til å beskytte verdifulle eiendeler og informasjon, opprettholde ansattes sikkerhet og øke den generelle tilliten og tryggheten.

Langsiktige fordeler, som forbedret effektivitet og kostnadsbesparelser, kan ta lengre tid å realisere. For eksempel kan et automatisert tilgangskontrollsystem strømlinjeforme prosessen med å kontrollere tilgangsrettigheter og tillatelser, redusere administrative kostnader og feil. Det kan også bidra til å unngå behovet for å ansette ekstra personell for å sikre begrensede områder. Disse fordelene kan legge seg opp over tid, noe som bidrar til løpende besparelser og økt effektivitet.

Samlet sett avhenger den forventede tidsrammen for å skape verdi med Facilities Access Control av den spesifikke implementeringen, størrelsen og kompleksiteten til anlegget og organisasjonens sikkerhets- og tilgangskontrollmål. Ikke desto mindre er tilgangskontroll en verdifull investering i å beskytte verdifulle eiendeler, informasjon og ansatte, og gi et trygt og sikkert miljø.

3.35 Administrasjon av fasiliteter

Mål

Målet med Facilities Management (FM) er å sikre at det bygde miljøet støtter effektiv funksjon av en organisasjons kjerneaktiviteter ved å tilby trygge, funksjonelle og komfortable fasiliteter. Spesielt kan målene for Facilities Management omfatte:

- Vedlikehold: Facility Management har som mål å sikre at det bygde miljøet vedlikeholdes, oppdateres og fornyes etter behov.
- Kostnadsoptimalisering: FM er opptatt av å optimalisere leveransen av fasilitetstjenester og oppnå valuta for pengene, samtidig som de sikrer at høye servicestandarder opprettholdes.
- Kapitalforvaltning: FM innebærer ofte å administrere de fysiske eiendelene til en organisasjon, inkludert bygningsstrukturer, utstyr og maskiner, sikre at de utnyttes optimalt og drive avkastning på investeringen.
- Bygningsytelse: Fasilitetsstyring fokuserer på å forbedre bygningens ytelsesstandarder som sikkerhet, energieffektivitet, miljøytelse og vedlikeholdseffektivitet.
- Beboertilfredshet og produktivitet: FM har som mål å gi et trygt og komfortabelt miljø for beboerne, fremme en følelse av velvære og engasjement med innendørs og utendørs arbeidsområder.

Oppsummert er målet med Facilities Management å administrere og optimalisere det bygde miljøet, støtte organisatoriske aktiviteter, øke verdien av fysiske eiendeler, optimalisere ressurser og sikre brukerkomfort og tilfredshet.

Forventet tidsramme for å skape verdi

Den forventede tidsrammen for å skape verdi fra Facilities Management avhenger av flere faktorer, inkludert tilstanden til den nåværende fasilitetsinfrastrukturen, organisasjonens mål og tilgjengeligheten av ressurser. Her er noen eksempler:

- Vedlikehold: Regelmessig vedlikehold av anleggets infrastruktur kan bidra til å forlenge levetiden, redusere nedetid og unngå kostbare reparasjoner. Verdien kan realiseres på kort til mellomlang sikt, avhengig av omfanget av nødvendig vedlikehold, kompleksiteten i systemene og tilgjengeligheten av ressurser.
- Forbedringer av energieffektivitet: Facility Management inkluderer ofte initiativer som tar sikte på å redusere energiforbruket og fremme bærekraftig praksis. Disse initiativene kan bidra til å redusere energikostnadene, forbedre miljøytelsen og oppfylle samsvarskrav. Verdien av energieffektivitetsforbedringer kan realiseres på mellomlang og lang sikt, da de ofte krever mer omfattende investeringer og implementering av komplekse løsninger.
- Bygningsytelse: Fasilitetsstyring innebærer også å forbedre bygningens ytelsesstandarder som sikkerhet, miljøytelse og vedlikeholdseffektivitet. Verdien av å bygge ytelsesforbedringer kan realiseres på lang sikt, da de ofte innebærer langsiktig planlegging, investering og implementering av løsninger.

Samlet sett varierer den forventede tidsrammen for Facilities Management for å skape verdi avhengig av de spesifikke målene og konteksten til organisasjonen. Et godt utført Facilities Management-program kan imidlertid gi umiddelbare fordeler som å redusere driftskostnader, forbedre sikkerheten og forbedre brukeropplevelsen, noe som kan resultere i langsiktige kostnadsbesparelser og produktivitetsforbedringer.

3.36 Fasilitetbruksdata

Mål

Bruksdata bidrar til å imøtekomme behovene til beboerne i ethvert arbeidsområde / område / anleggsrom ved å levere informasjon til anleggsadministrasjonsteamet som påvirker rengjøring på forespørsel, hot desking etc., etterfylling av forsyninger i ofte brukte områder som kaffehjørner.

Enheter som rapporterer til et skybasert overvåkingssenter som teller innkommende og utgående persontrafikk i en bestemt bygning eller steder for at ledelsen skal ta informerte beslutninger for ansettelsesledelsen, salgsomsetningen, suksessen til markedsføringskampanjen osv.

Forventet tidsramme for å skape verdi

Beleggsdata kan skape verdi umiddelbart fra implementeringstidspunktet. Verdien som skapes kan imidlertid variere avhengig av beleggsdataene, anleggets type og hvordan beleggsdataene analyseres og brukes.

Noen fordeler som kan realiseres umiddelbart etter implementering inkluderer:

- Effektivitet: Bruksdata for fasiliteter kan hjelpe organisasjoner med å identifisere underutnyttede områder og optimalisere bruken av dem. Dette kan redusere energisløsing og vedlikeholdskostnader.
- Produktivitet: Bruk av bruksdata for å forstå plassutnyttelse kan gi innsikt i effektiviteten til samarbeidsområder, gi ansatte rom som hjelper produktiviteten og skaper en atmosfære for å komme i sonen.
- Kostnadsreduksjon: Nøyaktige bruksdata forbedrer beslutningstaking, slik at bedrifter kan redusere størrelsen og utgiftene til fasiliteter som er underutnyttet.
- Miljøfordeler: Effektiv bruk av bruksdata kan redusere karbonutslipp og fremme miljømessig bærekraft.

Verdien av bruksdata fortsetter å utvikle seg over tid. Med kontinuerlig datainnsamling og analyse kan bruksdata brukes til å optimalisere plassutnyttelsen, utlede etterspørselsmønstre og redusere kostnadene. Dessuten, ettersom data fra flere nettsteder aggregeres, kan bredere innsikt genereres om bruksmønstre på tvers av ulike fasiliteter.

Samlet sett avhenger den forventede tidsrammen for å skape verdi fra bruksdata av ulike faktorer, inkludert størrelsen og kompleksiteten til fasiliteter, de analytiske verktøyene som brukes, og organisasjonens interne kultur mot datadrevet beslutningstaking.

3.37 Sammenligning av filer

Mål

Målet med filsammenligning er å finne og fremheve forskjellene mellom innholdet i to eller flere filer. Filene kan være i forskjellige formater, for eksempel tekstdokumenter, regneark eller programmer. Filsammenligning gjøres vanligvis for å:

- Bekreft nøyaktighet: Sammenligning av filer kan bidra til å validere at data er importert eller eksportert riktig. Hvis du for eksempel sammenligner en kildefil med en målfil etter dataoverføring, kan det bidra til å bekrefte at alle dataene er overført nøyaktig.
- Sikre konsistens: Sammenligning av flere versjoner av en fil kan bidra til å sikre konsistens på tvers av de forskjellige versjonene. For eksempel kan sammenligning av to versjoner av et program bidra til å identifisere eventuelle forskjeller eller feil i koden.
- Identifiser endringer: Sammenligning av to versjoner av et dokument kan bidra til å identifisere endringer som er gjort mellom dem. Dette kan være nyttig for å spore revisjoner, samarbeide om dokumenter eller for å identifisere plagiat.

- Løs konflikter: Sammenligning av to forskjellige versjoner av en fil kan bidra til å oppdage eventuelle konflikter mellom dem, for eksempel når du slår sammen kodeendringer som er gjort av forskjellige utviklere i et versjonskontrollsystem.

Samlet sett er målet med filsammenligning å sikre at filene er riktige, konsistente og oppdaterte, og å identifisere eventuelle endringer eller feil som kan eksistere mellom flere versjoner av en fil.

Forventet tidsramme for å skape verdi

Den forventede tidsrammen for å skape verdi fra filsammenligning avhenger av de spesifikke målene og konteksten. Her er noen eksempler:

- Sammenligning av programvarekode: I dette tilfellet kan filsammenligning bidra til å identifisere problemer og inkonsekvenser i kode, noe som hjelper til med feilsøking og testing. Verdien kan realiseres relativt raskt, avhengig av kodens kompleksitet og antall filer som må sammenlignes.
- Sammenligning av datafiler: Sammenligning av datafiler kan bidra til å sikre datanøyaktighet og kontrollere datakvaliteten. Forventet tidsramme for å opprette verdi avhenger av størrelsen på datafilene, kompleksiteten i sammenligningsprosessen og valideringsnivået som trengs.
- Sammenligning av dokumentversjoner: Sammenligning av dokumentversjoner kan bidra til å identifisere endringer som er gjort av forskjellige forfattere og sikre konsistens på tvers av versjoner. Forventet tidsramme for å opprette verdi avhenger av dokumentets kompleksitet og antall versjoner som må sammenlignes.

Samlet sett kan den forventede tidsrammen for å skape verdi fra filsammenligning variere mye avhengig av det spesifikke brukstilfellet og kompleksiteten til filene som sammenlignes. Filsammenligning kan imidlertid gi umiddelbare fordeler, for eksempel å identifisere feil eller inkonsekvenser, som kan føre til tids- og kostnadsbesparelser på lengre sikt.

3.38 Fillagringssystem ved hjelp av hybrid kryptografi cloud computing

Mål

Skyteknologi har blitt brukt på flere felt, produksjons- og forsvarsakademier, for å levere enorme mengder informasjon. Informasjon hentet fra skyen på forespørsel fra kunden. En rekke utfordringer bør løses for å holde informasjon i systemet. For å lagre data i skyen er det flere utfordringer som må løses. En rekke teknikker kan brukes i konfliktløsning. I denne artikkelen foreslo vi en hybrid steganografi og krypteringsmetode for datasikkerhet. I Internett-applikasjoner var bruken av en optimal løsning ikke egnet for informasjonsbeskyttelse på høyt nivå. Vi introduserte en ny sikkerhetsteknikk for symmetrisk nøkkelkryptografi og steganografi. Rivest chiffer 6 (RC6), Advanced Encryption Standard (AES), Byte Rotation

Algorithm (BRA) og blowfish teknikker for å gi blokk sikkerhetsinformasjon og lengden på den tekniske nøkkelen var 128 bits. En kritisk datasikkerhet, Least Signification Bit (LSB)Steganography-algoritmen ble brukt.

Forventet tidsramme for å skape verdi

1 – 3 måneder

3.39 Håndtering av trafikktopper

Mål

Målet med å håndtere trafikktopper er å sikre at nettstedet eller applikasjonen din kan håndtere plutselige økninger i trafikken uten å bremse eller krasje.

Forventet tidsramme for å skape verdi

Tiden det tar å skape verdi fra håndtering av trafikktopper, avhenger av infrastrukturens kompleksitet, antall brukere og organisasjonens spesifikke mål. Organisasjoner kan imidlertid se umiddelbare fordeler i form av forbedret ytelse og pålitelighet.

3.40 Vert for et statisk nettsted ved hjelp av AWS (eller andre skyer)

Mål

Trenden med hosting statiske nettsteder på Amazon S3 er en blir svært populær. Denne tilnærmingen har blitt tatt i bruk av mange organisasjoner på grunn av fordelene i forhold til tradisjonell serverbasert hosting. Statiske nettsteder er nettsteder som ikke krever noe kjøretidsmiljø som JRE, .NET, etc. og er for det meste basert på HTML, CSS, JS og andre statiske ressurser (lyd / videofiler, dokumenter, etc.). AWS tilbyr alle nødvendige tjenester og verktøy som lar deg bygge og administrere statiske nettsteder på AWS-skyen veldig enkelt. Li ke andre skybaserte hostings, det er ingen CAPEX-investering. Det er imidlertid en ubetydelig driftskostnad for hosting av det statiske nettstedet.

Forventet tidsramme for å skape verdi

1 – 3 måneder

3.41 Programmer for direktemeldinger

Mål

Direktemeldingsteknologi (IM) er en type online chat som tillater tekstoverføring i sanntid over Internett eller et annet datanettverk. Meldinger overføres vanligvis mellom to eller flere parter, når hver bruker skriver inn tekst og utløser en overføring til mottakeren (e), som alle er koblet på et felles nettverk. Det skiller seg fra e-post ved at samtaler over direktemeldinger skjer i sanntid (derav "øyeblikkelig"). De fleste moderne direktemeldingsprogrammer (noen ganger kalt "sosiale budbringere", "meldingsapper" eller "chat-apper") bruker push-teknologi og legger også til andre funksjoner som emojis (eller grafiske smilefjes), filoverføring, chatbots, voice over IP eller videochatfunksjoner.

Målet med direktemeldingsapplikasjoner er å gjøre det mulig for brukere å sende og motta meldinger umiddelbart i sanntid. Disse applikasjonene lar brukerne kommunisere med hverandre uavhengig av hvor de befinner seg, noe som gjør det praktisk og effektivt for folk å holde kontakten. Noen av de viktigste målene for direktemeldingsprogrammer inkluderer:

- Kommunikasjon: Det primære målet med direktemeldingsapplikasjoner er å gi brukerne en plattform for å kommunisere med hverandre i sanntid, enten via tekstmeldinger, taleanrop eller videosamtaler.
- Bekvemmelighet: Direktemeldingsprogrammer er utformet for å gi et mer praktisk og tilgjengelig kommunikasjonsmiddel enn tradisjonelle metoder som e-post eller telefonsamtaler.
- Tilkobling: Direktemeldingsprogrammer lar folk holde kontakten med hverandre til tross for at de er på forskjellige steder og tidssoner.
- Hastighet: Direktemeldingsprogrammer er designet for å fungere i sanntid, slik at brukerne kan sende og motta meldinger umiddelbart, noe som gjør kommunikasjonen raskere og mer effektiv.
- Personvern: Direktemeldingsprogrammer tilbyr ulike personvernfunksjoner, for eksempel ende-til-ende-kryptering, for å beskytte brukerdata og samtaler mot uautorisert tilgang.

Totalt sett er målet med direktemeldingsprogrammer å gjøre det mulig for folk å holde kontakten og kommunisere med hverandre raskt, praktisk og sikkert, uansett hvor de befinner seg.

Forventet tidsramme for å skape verdi

Direktemeldingsprogrammer kan skape verdi fra det øyeblikket de distribueres og bli utbredt av brukere. Verdien som direktemeldingsprogrammer tilbyr, er deres evne til å koble mennesker sammen og gjøre dem i stand til å kommunisere effektivt i sanntid. Jo flere som bruker disse applikasjonene, jo mer verdi gir de.

I mange tilfeller kan direktemeldingsapplikasjoner skape verdi i løpet av få minutter, så snart brukerne begynner å bruke plattformen til å få kontakt med hverandre. For eksempel kan en gruppe venner laste ned

et direktemeldingsprogram, opprette en gruppechat og begynne å bruke den til å holde kontakten. I dette scenariet opprettes verdien nesten umiddelbart.

I forretningssammenheng kan direktemeldingsprogrammer ta litt lengre tid å skape verdi, da de kan kreve integrasjon med andre forretningssystemer, sikkerhetsbekreftelse og adopsjon blant ansatte. Når applikasjonen er fullt implementert, kan den imidlertid gi betydelig verdi ved å gjøre det mulig for ansatte å kommunisere mer effektivt, samarbeide om prosjekter og svare raskere på kunder.

Samlet sett vil den forventede tidsrammen for et direktemeldingsprogram for å skape verdi variere avhengig av situasjonen og konteksten der den distribueres. Generelt kan imidlertid direktemeldingsprogrammer skape verdi relativt raskt ved å gjøre det mulig for folk å holde kontakten og kommunisere effektivt i sanntid.

3.42 Administrere virtuelt nettverk

Mål

Målet med å administrere virtuelle nettverk er å opprette, konfigurere og vedlikeholde en virtualisert nettverksinfrastruktur som kobler virtuelle maskiner (VM-er) og andre ressurser i skyen.

Forventet tidsramme for å skape verdi

Tiden det tar å skape verdi fra å administrere virtuelle nettverk, avhenger av kompleksiteten i nettverket, antall tilkoblede ressurser og organisasjonens spesifikke mål. Imidlertid kan virtuelle nettverk gi umiddelbare fordeler i form av forbedret skalerbarhet, fleksibilitet og sikkerhet.

3.43 Migrer til skyen

Mål

Målet med å overføre til skyen er å flytte organisasjonens programmer, data og infrastruktur fra lokale servere til en skybasert infrastruktur. Målet er å forbedre smidigheten, redusere driftskostnadene, forbedre skalerbarheten og forbedre sikkerheten.

Forventet tidsramme for å skape verdi

Tiden det tar å skape verdi fra migrering til skyen, avhenger av flere faktorer, inkludert kompleksiteten i den eksisterende IT-infrastrukturen, omfanget av overføringen og mengden ressurser som er tildelt prosjektet.

Mange organisasjoner ser imidlertid betydelige fordeler i form av forbedret smidighet, skalerbarhet og reduserte driftskostnader kort tid etter migrering til skyen.

3.44 Overvåking av aktivitetene som utføres av landbruksmaskiner på en gitt overflate

Mål

Landbruksarbeidet som utføres av maskinene som kjøres av sjåføren er stressende og krever ofte mye av sjåføren. Disse tingene skyldes det faktum at repeterende operasjoner utføres ofte og noen ganger under vanskelige værforhold (ekstreme temperaturer, høy luftfuktighet, etc.) Føreren av disse maskinene fungerer noen ganger under vanskelige forhold på grunn av årsakene vist ovenfor. Det er for få muligheter til å forbedre arbeidsforholdene til sjåføren.

Landbruksmaskiner som fungerer uten å bli drevet direkte av mennesker ser ut til å være en moderne og levedyktig løsning. I dette tilfellet brukes kunstig intelligens og robotteknologi for å øke ytelsen til disse maskinene. Den foreslåtte søknaden overvåker aktiviteten til en eller flere maskiner som arbeider på en grunnflate.

Forventet tidsramme for å skape verdi

Måneder – 12 måneder

3.45 Overvåking av de fysiologiske parametrene til idrettsutøvere under trening

Mål

Idrettsutøveres trening er alltid ledsaget av endringer i verdiene til noen fysiologiske parametere. Målingen av disse parametrene og deres påfølgende behandling gir data om hvordan utøverens kropp reagerer på kravene under trening.

Overskridelse av et visst etterspørselsnivå kan føre til ulykker. Søknaden foreslår å overvåke noen fysiologiske parametere for idrettsutøvere under trening.

Forventet tidsramme for å skape verdi

3 uker – 4 måneder

3.46 Drive flere prosjekter samtidig

Mål

Målet med å drive flere prosjekter samtidig ved hjelp av Google Cloud Platform er å administrere flere prosjekter effektivt og utnytte skalerbarheten, sikkerheten og kostnadseffektiviteten til Google Cloud Platform.

Forventet tidsramme for å skape verdi

Tiden det tar å skape verdi fra å drive flere prosjekter samtidig ved hjelp av Google Cloud Platform, avhenger av kompleksiteten til prosjektene, antall ressurser som er involvert, og organisasjonens spesifikke mål. Organisasjoner kan imidlertid se umiddelbare fordeler i form av forbedret effektivitet, ressursutnyttelse og prosjektresultater.

3.47 Rekonfigurering av offentlige transportruter i en by

Mål

Midlene til offentlig transport i en lokalitet har en veldefinert rute som de dekker med bestemte tidsintervaller i henhold til en fastsatt tidsplan. I rushtiden er kollektivtransportmidlene mer overbelastet, og resten av dagen lastes transportmidlene langt under sin nominelle kapasitet (antall transporterte).

Applikasjonen omkonfigurerer sirkulasjonsveien til kollektivtransportmidlene slik at de sirkulerer lastet nær sin normale kapasitet og oppfyller kravene fra reisende.

Forventet tidsramme for å skape verdi

3 måneder - 2 måneder

3.48 Fjernstyrte smarte enheter i smarte hjem / kontor

Mål

Denne studien diskuterer virkningen av omgivelsesforholdstiltak på kundeatferd og dens anvendelse i detaljhandelen. Det presenteres grunnleggende datasettstruktur som består av respektive datakilder, nemlig IoT-sensorer, smarte målere og interne transaksjons- og analytiske databaser, og forretningsindikatorer som brukes til å optimalisere undermiljøer for luftkvalitet i butikkene. Maskinlæring foreslås for å automatisere

kunnskapsoppdagelse og mønsteroppdagelse fra data og som grunnlag for et grensesnitt til interoperabelt klimaanlegg.

Forventet tidsramme for å skape verdi

6 - 9 måneder

3.49 Administrasjon av ressurs- og programtilgang

Mål

Bruk av IAM-tjenestene for å holde oversikt over hvem som har tilgang til hvilke ressurser og apper.

Ved hjelp av den rollebaserte tilgangskontrollen (RBAC) i Azure Active Directory (AD) kan du konfigurere tillatelsene for brukere i en organisasjon, definere hvem som har tilgang til hva ved å godkjenne dem med Azure AD-legitimasjon og deretter godkjenne dem ved å sammenligne rollene brukeren har, og tillatelsene som er konfigurert for et bestemt program eller en bestemt ressurs. Dette gjør det mulig å sette opp en policy med minst privilegium.

For å øke sikkerheten implementere ulike måter å autentisere brukeren på, for eksempel flerfaktorautentisering (MFA), der du mottar et engangspassord på enheten din, eller biometri, der du bruker ansiktsgjenkjenning eller fingeravtrykk for å autentisere.

Når brukeren er godkjent, slår IAM-tjenesten opp brukerens roller, det være seg den permanente rollen eller JIT-rollen (Just-In-Time) som er gitt gjennom PIM (Privileged Identity Manager), og sammenligner den med tilgangspolicyen som er konfigurert på ressursen eller programmet som brukeren prøver å få tilgang til.

Konfigurere enhetsidentiteten Du kan også kontrollere at enheten brukeren bruker for øyeblikket, anses som sikker ved å bruke betinget tilgang. Dette kan også konfigureres til å bare tillate tilgang fra bestemte steder, for eksempel innenfor et bestemt IP-sted, innenfor bestemte tidsrammer eller bruke risikodeteksjon for å avgjøre om brukeratferden anses som uvanlig.

Du kan overvåke bruken og gi autorisasjon til bestemte brukere for å klargjøre eller fjerne ekstra ressurser. Det brukes også til å se hvilke brukere som har tilgang til en bestemt ressurs eller app på et bestemt tidspunkt, noe som kan bidra til å feilsøke hvor et datainnbrudd har skjedd.

Forventet tidsramme for å skape verdi

3 uker – 1 måned

3.50 Regelbasert klassifisering av phishing-webområder

Mål

I disse dager gjennomsøker forskjellige roboter Internett, de kalles også: bots, harvesters eller spiders. Populære søkemotorer bruker en lignende teknikk for å indeksere nettsider - de har en autonom agent (kalt robot eller bot) som har ansvaret for å gjennomsøke ulike attributter til nettsteder. I det siste har denne crawlerteknikken blitt utnyttet av ondsinnede brukere, for eksempel harvesters, som brukes til å skrape e-postadresser fra nettsteder for å bygge en spam-liste for epost-spammere. Nylig er roboter også misbrukt til å kjøpe flybilletter eller gjøre raske bud i on-line auksjonssystem. I dette papiret presenterer vi et intelligent system kalt Lino som prøver å løse det nevnte problemet. Lino er et system som simulerer en sårbar nettside og fanger webcrawlere. Vi samler inn ulike funksjoner og utfører en prosedyre for funksjonsvalg for å finne ut hvilke funksjoner som hovedsakelig bidrar til klassifisering av besøkendes atferd. For klassifiseringsformålet bruker vi toppmoderne maskinlæringsmetoder som Support Vector Machine og beslutningstre C 4.5.

Forventet tidsramme for å skape verdi

1 – 3 måneder

3.51 SAP Build

Mål

Hovedmålet med SAP Build er å gjøre det mulig for forretningsbrukere og andre interessenter å enkelt og raskt lage brukergrensesnitt og andre applikasjoner uten å kreve tekniske ferdigheter. SAP Build er en skybasert plattform som gir et dra-og-slipp-grensesnitt der brukere enkelt kan lage og designe nettbaserte applikasjoner.

SAP Builds primære mål er å redusere tiden og innsatsen som kreves for å designe og utvikle brukergrensesnitt, noe som vanligvis er en kompleks og tidkrevende prosess. Det gir et brukervennlig samarbeidsmiljø der forretningsbrukere enkelt kan opprette, visualisere og teste applikasjonsideene sine uten å kreve hjelp fra tekniske utviklere.

SAP Build er designet for å forbedre den generelle brukeropplevelsen og brukergrensesnittdesignen til SAP-applikasjoner. Det gir en rekke maler, designelementer og mønstre som lar brukerne raskt lage intuitive, brukervennlige grensesnitt som er i samsvar med SAPs designprinsipper.

Samlet sett er målet med SAP Build å gi forretningsbrukere og andre interessenter mulighet til å ta en aktiv rolle i design og utvikling av brukergrensesnitt, slik at applikasjonene oppfyller deres behov og krav, samtidig som de overholder beste praksis innen UI-design og utvikling.

Forventet tidsramme for å skape verdi

Tidsrammen for å skape verdi ved hjelp av SAP Build avhenger av ulike faktorer som kompleksiteten i brukergrensesnittet, tilgjengelige ressurser og kompetansenivået til teamet som utvikler applikasjonen. Bruken av SAP Build kan imidlertid redusere tiden og innsatsen som kreves for å designe og utvikle brukergrensesnitt, noe som gir raskere tid til markedet for applikasjoner.

Vanligvis, med SAP Build, kan brukere lage interaktive prototyper og utføre brukertesting i løpet av noen uker, noe som bidrar til å identifisere eventuelle designproblemer tidlig og sikrer at den endelige applikasjonen oppfyller brukerens behov.

Bruken av SAP Build kan også forbedre brukertilfredsheten og produktiviteten ved å skape mer intuitive og brukervennlige grensesnitt, noe som resulterer i en mer strømlinjeformet arbeidsflyt og bedre brukeropplevelse.

Samlet sett kan verdien av SAP Build være umiddelbart tydelig, spesielt når det gjelder å redusere tiden og innsatsen som trengs for å designe og utvikle brukergrensesnitt, forbedre brukertilfredsheten og produktiviteten, og muliggjøre en raskere time-to-market for applikasjoner. Den forventede tidsrammen for å skape verdi vil bli bestemt av organisasjonens spesifikke mål og designbehov.

3.52 Definere lastbalanseringer

Mål

Under toppbelastningstider kan serverne få mer trafikk enn de er i stand til å håndtere, noe som fører til tapte pakker, tap av data og applikasjoner som ikke svarer som igjen kan føre til tap av brukere. Å sette opp en automatisk lastbalansering vil løse dette problemet ved å distribuere den innkommende trafikken på flere servere, slik at ingen enkelt server blir overbelastet og blir til en flaskehals. Dette forbedrer den generelle ytelsen, tilgjengeligheten og skalerbarheten som kjøres i skyinfrastrukturen.

Forventet tidsramme for å skape verdi

Umiddelbar

3.53 Smart trafikkstyring

Mål

Prosjektet løser problemet med det økende behovet for sikkerhet (spesielt i offentlige rom) og trafikkregulering i dag, retningen på hvordan området utvikler seg og hva behovene vil være i nær fremtid. Løsningen på problemet vil oppnås ved å utvikle en plattform som ved hjelp av avanserte maskinlæringsteknologier transformerer overvåkings- og kontrollsystemer til verktøy som åpner applikasjonsmuligheter innen smart trafikk og sikkerhet.

Utfordringene til andre systemer på markedet ses gjennom: (i) på den ene siden av markedet finnes det løsningsleverandører som oftest sender et budskap om at deres løsninger støtter en helhetlig tilnærming til overvåking/sikkerhet og trafikk/transport på beste praksis-måte. Disse løsningene inkluderer bare et grunnleggende eller redusert antall funksjoner, og er vanskelig / umulig å støtte interoperabilitet av det systemet med andre som brukeren har. Slike løsninger har en vektlagt orientering mot en bestemt (en) produsent, demonstrerer vanskelig overgang til andre løsninger når den spesifikke løsningen er introdusert og er vanligvis kostbar når det gjelder utvikling og innføring av det grunnleggende systemet samt enhver integrasjon eller overbygning ("overprising" / "over-løfte" problem); (ii) På den andre siden viser små utfordrere på markedet potensial ved å bruke fremskritt innen teknologier (krets- og programvarestøtte, dvs. matematiske modeller), men de klarer vanligvis ikke å skalere løsninger eller sikre en høyere grad av markedsandel på grunn av de høye kostnadene ved å utvikle grunnleggende funksjonaliteter, dvs. det faktum at den grunnleggende investeringen i utvikling for å kunne tilby selv det laveste servicenivået, det må være stort ("laboratorietilnærming" -problem); (iii) selv om de presenteres som sådan, er konkurranseløsninger sjelden optimalisert innen overvåking / sikkerhet og transport / logistikk med fravær av klare mønstre eller studier der interoperabilitet mellom ulike systemer utføres og så mange brukere som mulig innen overvåking / sikkerhet og transport / logistikk anser det nødvendig fordi de over tid har investert betydelige ressurser i ulike teknologier; (iv) personvernkontroll er også et logisk krav, som i størst grad innebærer kontroll over modellene som fører til bestemte handlinger eller er grunnlaget for å forstå atferd innen overvåking/sikkerhet og transport/logistikk; (v) Til slutt er løsninger innen overvåking / sikkerhet og transport / logistikk ofte under spesielle lovbestemmelser og er gjenstand for endringer i dem, noe som øker behovet for tilpasning gjennom modellkorreksjon og konstruksjon av slike systemer på åpne teknologier med høy grad av kontroll over modellene som fører til innsikt.

Forventet tidsramme for å skape verdi

12 - 24 måneder

3.54 Levere salgsdata i sanntid

Mål

For å kunne bruke den innsamlede informasjonen til å gjøre endringer i kampanjer, prøve nye kampanjer og endre dem basert på kontinuerlig tilbakemelding eller distribuere ansatte over flere steder for å planlegge for topper i arbeidet som må gjøres.

Forventet tidsramme for å skape verdi

6 måneder – 12 måneder

3.55 Det grafiske grensesnittet for programmering på en biltjeneste kombinert med et nettsted

Mål

Selskaper som tilbyr tjenester til befolkningen som biltjenester, private medisinske kontorer, etc. Han planlegger sin aktivitet daglig, med tanke på tiden som trengs for å utføre en aktivitet.

For eksempel, hvis en persons bil har et problem, må eieren av bilen gå til et verksted for å diagnostisere bilen, foreslå metoder for å rette opp situasjonen og fikse feilen.

Denne applikasjonen gir kunden muligheten til online planlegging hos en biltjeneste for å diagnostisere feilen til en bil.

Forventet tidsramme for å skape verdi

2 uker – én måned

3.56 Videokonferanse system

Mål

Målet med et videokonferansesystem er å muliggjøre ekstern kommunikasjon og samarbeid mellom mennesker eller team, uavhengig av deres fysiske plassering. Spesielt kan målene for et videokonferansesystem omfatte:

- Sanntidskommunikasjon: Et videokonferansesystem har som mål å gi en plattform for sanntids, ansikt til ansikt-interaksjon mellom deltakerne, slik at eksterne team eller enkeltpersoner kan kommunisere naturlig og effektivt.
- Samarbeid: Et videokonferansesystem kan lette samarbeidet ved å la deltakerne dele filer, dokumenter og skjermer, redigere dokumenter samtidig og til og med idédugnad over virtuelle tavler.
- Bekvemmelighet: Et videokonferansesystem tar sikte på å gi bekvemmelighet og fleksibilitet ved å eliminere behovet for at deltakerne er fysisk til stede på samme sted, slik at de kan delta i møter fra hvor som helst i verden.
- Tidsbesparelser: Et videokonferansesystem kan bidra til å spare tid ved å unngå behovet for reiser og redusere nedetid mellom møter, slik at deltakerne kan holde seg produktive og engasjerte.
- Kostnadsbesparelser: Et videokonferansesystem kan bidra til å spare kostnader forbundet med reise og opphold, spesielt for organisasjoner med flere kontorer på forskjellige steder eller for eksterne team som ellers ville kreve kontorlokaler for å jobbe.

Totalt sett har et videokonferansesystem som mål å gi en sømløs og effektiv måte for eksterne team eller enkeltpersoner å kommunisere og samarbeide på, noe som forbedrer produktiviteten, bekvemmeligheten og kostnadsbesparelsene.

Forventet tidsramme for å skape verdi

Den forventede tidsrammen for å skape verdi fra et videokonferansesystem avhenger av ulike faktorer, for eksempel størrelsen på organisasjonen, dens operasjonelle struktur, hyppigheten av møter og teknologiøkosystemet. Her er noen generelle eksempler:

- Forbedret samarbeid: Videokonferansesystemer kan forbedre samarbeidet ved å tilby video- og lydfunksjoner i sanntid, noe som gjør det enklere for team å samarbeide eksternt. Verdien av denne funksjonen kan realiseres på kort sikt, selv under de første videokonferansene.
- Reduserte reiseutgifter: Videokonferansesystemer kan spare reisekostnader ved å erstatte personlige møter med virtuelle, noe som fører til reduserte reiseutgifter, for eksempel fly, overnatting og transport. Verdien av reduserte reiseutgifter kan realiseres umiddelbart, i løpet av de første videokonferansene eller møtene der reiser unngås.
- Raskere beslutningstaking: Videokonferansesystemer kan bidra til raskere beslutningstaking ved å gi øyeblikkelig video- og lydtilgang, som støtter beslutningstaking i sanntid. Verdien av raskere beslutningstaking kan realiseres umiddelbart og gjennom langsiktig bruk av systemet.

Samlet sett kan den forventede tidsrammen for å skape verdi fra et videokonferansesystem være umiddelbar, spesielt når det gjelder kostnadsbesparelser fra reduserte reiseutgifter og forbedret samarbeid. Tilleggsverdi kan materialisere seg på mellomlang og lang sikt ettersom organisasjonen utvikler et stabilt økosystem med velbygde prosesser og teknologi for å støtte møter og samarbeid.

3.57 VoD-tilbud

Mål

Med Video on Demand (VoD) kan du opprette et bibliotek med videoer som brukerne dine har tilgang til når som helst. Du kan også kontrollere tilgangen til videoene dine ved å angi hvem som kan se dem, og når. Azure Media Services (AMS) tilbyr også verktøy som hjelper deg med å administrere videoinnholdet ditt, inkludert indeksering, søk og analyse.

Hvis du vil bruke AMS VoD, må du først laste opp videoene til plattformen. Du kan gjøre dette gjennom AMS-portalen, REST API-er eller gjennom en rekke tredjepartsverktøy og -tjenester. Når videoene dine er lastet opp, kan du bruke AMS til å kryptere dem til forskjellige formater, opprette flere bithastigheter og kryptere dem for sikker levering.

Etter at videoene dine er behandlet, kan du bruke AMS-spilleren til å legge dem inn på nettstedet eller appen din. Spilleren støtter en rekke funksjoner, inkludert adaptiv streaming, teksting og flere lydspor. Du kan også tilpasse spillerens utseende og følelse for å matche merkevaren din.

Forventet tidsramme for å skape verdi

2 måneder – 4 måneder

3.58 Vannforsyningsstyring ved hjelp av avstandslesere i vannforsyningsnett

Mål

Digital transformasjon muliggjør betydelige besparelser gjennom ressursstyring og forbedring av forretningsprosesser. Det endrer måten vi bruker informasjonen vi har, typen og mengden data vi kan samle inn. For å gjøre disse dataene mer anvendelige, bruker vi moderne analyse- og visualiseringsverktøy hvis oppgave er å få nyttig og rettidig informasjon fra en stor mengde forskjellige data på en enkel og fleksibel måte.

Problemene som oppstår i dette interesseområdet spenner fra hvordan man visualiserer data, hvilke metoder som skal brukes til å finne kunnskap skjult i data, og hvordan man utvikler prognosemodeller ved hjelp av data.

Forskere og industri har spesielt fokus på værdata som kan ha betydning

innvirkning på prediksjon i tider med uforutsigbare klimaendringer og værpåvirkninger. I tekniske spørsmål for bedrifter som ønsker å gjøre det første skrittet i dette området, er de møter spørsmål fra hvordan å lagre data i en "sky" / "big data" container, er det mulig å utvikle data prosjekt som "vokser sammen med et selskap" og mer og mer innhentede data, om det kan alle arbeide i sanntid og er denne "pakken" tilgjengelig for dem i form av kostnader og kunnskap som trengs.

Forventet tidsramme for å skape verdi

6 – 9 måneder

3.59 Webapplikasjon for online fullføring av selskapets ansattes timeliste

Mål

Byggefirmaer utfører arbeid på ulike arbeidspunkter som ligger i et geografisk rom. Hvert arbeid blir deltatt av frittliggende lag i løpet av arbeidet.

På selskapets hovedkontor må det føres oversikt over arbeidstiden til hvert medlem av arbeidsteamet. Søknaden gjør at oppmøtet kan fullføres oppdatert for hvert medlem av lagene som utfører sin aktivitet på forskjellige arbeidspunkter.

Forventet tidsramme for å skape verdi

3 uker - 1 måned

3.60 Nettsted hosting med statisk innhold

Mål

Å ha et nettsted er avgjørende for enhver bedrift i dag for å være konkurransedyktig. Det gir virksomheten muligheten til å opprettholde en online tilstedeværelse for sine potensielle kunder og brukere, noe som gir virksomheten 24/7 tilgjengelighet, synlighet og tilgjengelighet for dine nåværende og potensielle nye brukere. Dette gir dem muligheten til å oppdage virksomheten din uten å være begrenset av ting som åpningstider, ventetider på telefon og å måtte besøke et fysisk sted.

Selv de enkleste nettstedene vil tillate virksomheten å gi informasjon til besøkende om ting som åpningstider på et bestemt sted, kontaktinformasjon eller informasjon om produktene eller tjenestene virksomheten tilbyr. Den kan også brukes til å vise videoer og bilder som markedsfører virksomheten og dens produkter / tjenester.

Dette betyr at å ha et nettsted potensielt kan gi en bedrift en global rekkevidde og tilstedeværelse, samtidig som det reduserer tid og kostnader brukt på kundeservice / support ved å ha mange vanlige spørsmål besvart på nettstedet. Og tilbyr en praktisk plattform for å engasjere seg med kunder / brukere ved å vise produkter og tjenester via reklamemateriell som videoer som er vert på nettstedet eller sende nyhetsbrev med eksklusive tilbud eller rabatter sendt direkte til interesserte kunder / brukere til et globalt publikum.

Forventet tidsramme for å skape verdi

1 uke – 6 måneder

3.61 Nettbutikk

Mål

Å selge produkter, enten det er online, på et mursteinsted eller begge deler, å ha tilgang til nøyaktig og samtidig informasjon om den nåværende tilstanden til produktbeholdningen din er viktig for å kunne gi best mulig opplevelse for en kunde og minimere risikoen for å gå tom for lager som kan føre til ordrebøker og misfornøyde kunder.

Å holde oversikt over kundene dine og bestillingene de har gjort er også viktig, da det både er viktig for å sikre at du kan gi riktig nivå av kundestøtte til kunden din, og det kan brukes til å få viktig innsikt i kundens oppførsel, for eksempel hva slags produkter de er interessert i som kan brukes til å lage skreddersydd innhold for kundene dine.

Forventet tidsramme for å skape verdi

2 uker – 2 måneder

LITTERATUR

1. Cloud Industry Forum. (2022). *8 kriterier for å sikre at du velger riktig skytjenesteleverandør.* Hentet fra https://cloudindustryforum.org/8-criteria-to-ensure-you-select-the-right-cloud-service-provider/
2. CloudSigma. (2023). *10 trinn for å velge den beste skyleverandøren.* Hentet fra https://www.cloudsigma.com/10-steps-to-choose-the-best-cloud-provider/
3. Føll. (2023). *Cloud connect forklart.* Hentet fra https://www.colt.net/resources/cloud-connect-explained/
4. CompTIA. (2022). *En hurtigstartguide for skynettverk: rundt nettverket i 8 trinn.* Hentet fra https://www.comptia.org/content/guides/cloud-network-setup-guide
5. CompTIA. (2023). *Delvis skyet med en sjanse for databehandling: En nybegynnerguide til skytyper, løsninger og leverandører.* Hentet fra https://www.comptia.org/content/articles/cloud-types-solutions-and-vendors
6. CompTIA. (N. A.). *Delvis overskyet med en sjanse for databehandling: En nybegynnerveiledning til skytyper, løsninger og leverandører.* Hentet fra https://www.comptia.org/content/articles/cloud-types-solutions-and-vendors
7. Delta. (2020). *Styrke konkurranseevnen i datasentre.* Hentet fra https://www.deltapowersolutions.com/en/mcis/technical-article-powering-competitiveness-in-datacenters.php
8. Dialogisk. (2017). *Introduksjon til Cloud Computing, hvitbok.* Hentet fra https://www.dialogic.com/~/media/products/docs/whitepapers/12023-cloud-computing-wp.pdf
9. Dialogisk. (2017). Introduksjon til Cloud Computing, hvitbok. Hentet fra https://www.dialogic.com/~/media/products/docs/whitepapers/12023-cloud-computing-wp.pdf
10. Eldh, E. (2013). *Skytilkobling for innebygde systemer (Master of Science Thesis).* Kungliga Tekniska Högskolan i Stockholm, Sverige.
11. Faddom. (2021). Cloud Computing Kostnader og prissammenligninger for 2023. Hentet fra https://faddom.com/cloud-computing-costs-and-pricing-comparison/
12. FERI. (2022). *Beregning av sky.* Hentet fra: https://moja.um.si/studijski-programi/Strani/ucnaenota.aspx?jezik=S&fakulteta=FERI&sifraue=61M252
13. FR. (2022). *Andre nivå Masterstudium Computing and Informatics Presentation Proceedings for studenter som først ble registrert i 1. år i studieåret 2022/2023 Ljubljana*. Hentet fra: chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/viewer.html?pdfurl=https%3A%2F%2Fwww.fri.uni-lj.si%2Fupload%2FZborniki%2F1000471_Ra%25C4%258Dunalni%25C5%25A1tvo_in_informa%2520-%2520Copy%252011.pdf&clen=765163&chunk=true.
14. Google Cloud. (2022a). *Cloud Interconnect-dokumentasjon.* Hentet fra https://cloud.google.com/network-connectivity/docs/interconnect
15. Google Cloud. (2022b). *Google Cloud-vilkår.* Hentet fra https://cloud.google.com/network-connectivity/docs/concepts/key-terms

16. ITPro i dag. (2022a). 2022 *Cloud Computing Trender.* Hentet fra https://www.youtube.com/watch?v=PiaouNqFNwA
17. ITRPro i dag. (2022b). *Tilbyderne fortsetter å dominere, ledet av AWS.* Hentet fra https://www.itprotoday.com/iaas-and-paas/big-3-public-cloud-providers-continue-dominate-led-aws#close-modal
18. ITU. (2012). *Teknisk rapport: Del 1: Introduksjon til skyøkosystemet: definisjoner, taksonomier, brukstilfeller og krav på høyt nivå.* Hentet fra https://www.itu.int/pub/T-FG-CLOUD-2012-P1
19. ITU. (2022). *Focus Group Cloud, Teknisk rapport, Del 1: Introduksjon til skyøkosystemet: definisjoner, taksonomier, brukstilfeller og krav på høyt nivå, versjon 1.0.* Hentet fra https://www.itu.int/pub/T-FG-CLOUD-2012-P1
20. Jones, E. (2022). *Cloud Market Share: En titt på Cloud Ecosystem i 2023*. Hentet fra https://kinsta.com/blog/cloud-market-share/
21. Letica, J. &; Buić, N. (2014). *Innovasjon i VET.* Hentet fra http://www.refernet.hr/media/1236/innovation-in-vet_croatia.pdf
22. Marinescu, D. (2017). *Cloud computing teori og praksis*. USA: Elsevier, Morgan Kaufmann forlag.
23. Markeder og markeder. (2019). Hentet fra https://www.marketsandmarkets.com/
24. Marko, K. (2021). *Skyleverandører kjemper om markedsandelen i 2021.* Hentet fra https://www.techtarget.com/searchcloudcomputing/opinion/Cloud-providers-jockey-for-market-share
25. Uttalelse fra Den europeiske økonomiske og sosiale komité om "Industri 4.0 og digital transformasjon: hvor du skal gå". (2016). Hentet fra: chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/viewer.html?pdfurl=https%3A%2F%2Feur-lex.europa.eu%2Flegal-content%2FEN%2FTXT%2FPDF%2F%3Furi%3DCELEX%3A52016AE1017%26from%3DEN&pdffilename=CELEX%3A52016AE1017%3AEN%3ATXT.pdf.
26. Orakel (2023). *Hva er kan databehandling?* Hentet fra https://www.oracle.com/cloud/what-is-cloud-computing/top-10-benefits-cloud-computing/
27. Peterson, R. (2023). *Cloud Computing Tutorial for nybegynnere: Hva er &; Arkitektur.* Hentet fra https://www.guru99.com/cloud-computing-for-beginners.html
28. Rathore, A. (2022). *Hvordan finne den beste skyserveren for små bedrifter?* Hentet fra https://kanakinfosystems.com/blog/best-cloud-server-for-small-business
29. Appellerer. (2020). *Hva er de forskjellige typene lastbalansere?* Hentet fra https://www.resonatenetworks.com/2020/05/25/what-are-the-different-types-of-load-balancers/
30. Richter, F. (2023). *De tre store dominerer det globale skymarkedet.* Hentet fra https://www.statista.com/chart/18819/worldwide-market-share-of-leading-cloud-infrastructure-service-providers/
31. Rosencrance, L. (2021). *Bryte ned kostnadene for cloud computing i 2023.* Hentet fra https://www.techtarget.com/whatis/Breaking-Down-the-Cost-of-Cloud-Computing

32. Samoshki, D. (n. d.). *Nettskyrapporten.* Hentet fra https://the-report.cloud/how-to-choose-a-cloud-for-your-business/
33. Sharma, M. (2023). *Lastbalansering i Cloud Computing.* Hentet fra https://www.geeksforgeeks.org/load-balancing-in-cloud-computing/
34. Sharwood, S. (2022). *Cloud et tre-spillers marked dominert av AWS, Google, Microsoft.* Hentet rom https://www.theregister.com/2022/05/02/cloud_market_share_q1_2022/
35. Slovensk smart spesialiseringsstrategi S4. (2017). Hentet fra: chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/viewer.html?pdfurl=https%3A%2F%2Fwww.gov.si%2Fassets%2Fvladne-service%2FSVRK%2FS4-Slovenian-strategy-smart-specialization%2FSlovenska-strategy-smart-specialization.pdf&clen=1536948.
36. Spaanenburg, L. & Spaanenburg, H. (2010). *Skytilkobling og innebygde sensoriske systemer*. New York: Springer.
37. Spaanenburg, L., Spaanenburg, H. (2010). *Skytilkobling og innebygde sensoriske systemer.* Sveits: Springer.
38. Spilka, S. (2021). *Cloud Pricing Models - Kaster lys over prisalternativer.* Hentet fra https://www.exoscale.com/syslog/cloud-pricing-models/
39. Et langsiktig samfunns strategi. (2017 extension://efaidnbmnnnibpcajpcglclefindmkaj/viewer.html?pdfurl=https%3A%2F%2Fwww.umar.gov.si%2Ffileadmin%2Fuser_upload%2Fpublikacije%2Fkratke_analize%2FStrategija_dolgozive_druzbe%2FStrategija_dolgozive_druzbe.pdf&clen=2707481&chunk=true).
40. Slovenias utviklingsstrategi 2030 (2017). Hentet fra: chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/viewer.html?pdfurl=https%3A%2F%2Fwww.gov.si%2Fassets%2Fvladne-sluzbe%2FSVRK%2FStrategy-development-Slovenije-2030%2FStrategija_razvoja_Slovenije_2030.pdf&clen=4124906.
41. Strategi for høyere yrkesfaglig utdanning i Republikken Slovenia for perioden 2020-2030. (2017). Hentet: chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/viewer.html?pdfurl=https%3A%2F%2Fwww.gov.si%2Fassets%2Fministrstva%2FMIZS%2FDokumenti%2FVisje-professional-education%2FStrategija-higher-professional-education-RS-2020-2030%2FStrategija-higher-professional-education-in-republic-slovenia-for-period-20202030.pdf&clen=1259647.
42. Suhag, A. (2020). *Hva er de forskjellige typene skylastbalansering?* Hentet fra https://www.cloudmanagementinsider.com/different-types-of-cloud-load-balancing/
43. Teknisk trakt. (2021). 14 utrolige fordeler med cloud computing for bedrifter. Hentet fra https://www.techfunnel.com/information-technology/benefits-of-cloud-computing/
44. Den komplette Cloud Computing Manual. (2022). Hentet fra https://online.fliphtml5.com/dslwu/jeti/
45. Tripney, S. &; Hombrados, J. (2013). Teknisk og yrkesrettet utdanning og opplæring (TVET) for unge i lav- og mellominntektsland: en systematisk oversikt og metaanalyse. *Tidsskrift for empirisk forskning i yrkesopplæring og opplæring, 5*(3), 1-14. DOI: 10.1186/1877-6345-5-3.

46. Velte, A. T., Velte, J. V., & Elsenpeter, R. (2010). *Cloud Computing: En praktisk tilnærming.* New York: McGraw-Hill.
47. Westlake. (2022). *Fordeler med cloud computing for bedrifter.* Hentet fra https://www.westlake-it.co.uk/news/2022/05/30/benefits-of-cloud-computing-for-businesses/
48. Wikipedia. (2022). *Border Gateway-protokollen.* Hentet fra https://en.wikipedia.org/wiki/Border_Gateway_Protocol
49. Kablet. (2020). *Datasentre sluker ikke planetens elektrisitet - ennå.* Hentet fra https://www.wired.com/story/data-centers-not-devouring-planet-electricity-yet/

VEDLEGG

Vedlegg 1: Den amerikanske presidentkampanjen i 2012 og hvordan AWS støttet Obama

I denne enheten vil vi se på hvordan Amazons cloud computing-teknologi tillot president Obamas presidentkampanje i 2012 å unngå en IT-investering som ville ha kommet opp i et titalls millioner dollar.

En titt på vår casestudie:

Kampanjens IT-team brukte AWS til å bygge, lansere, kjøre og utvide appene sine. Etter valget lastet de alt opp til Amazon S3 og skalerte langt ned. De opprettet og drev over 200 AWS-apper som kunne håndtere millioner av mennesker. På de siste fire dagene av kampanjen håndterte en av disse applikasjonene, kampanjeanropsverktøyet, 7000 samtidige brukere og foretok over to millioner samtaler.

Hvorfor bruke AWS?

Her er 3 viktige aspekter som påvirket hvorfor AWS ville bli brukt som cloud computing-leverandør i Obama-kampanjen:

1. Sikkerhet og samsvar

Valg tiltrekker seg noen av verdens mest aggressive trusler mot informasjonssikkerhet. Når det gjelder valgteknologi, er informasjonssikkerhet en viktig prioritet. AWS forstår valgadministratorers ansvar og oppfyller eller overgår sikkerhets- og samsvarsstandarder på alle nivåer av kundenes skyreise. AWS prioriterer datasikkerhet, og vår verdensomspennende infrastruktur er utviklet og administrert i samsvar med beste praksis for sikkerhet.

2. Velgerengasjement

I 2018 var alle millennials (de i alderen 18 til 29) kvalifisert til å stemme i USA for første gang. Millennials foretrekker transaksjoner på nettet og har høye forventninger til skreddersydde kundeopplevelser. AWS tilbød byggeklosser som raskt kan settes sammen for å støtte praktisk talt enhver sikker arbeidsbelastning for målrettet oppsøking.

3. Valgadministrasjon

Valgadministrasjon refererer til kontor-oppgaver som velgerregistrering som fungerer som drivere for driftseffektivitet på tvers av flere sammenkoblede systemer, applikasjoner og lokale organisasjoner som spenner over fylker og distrikter. AWS tilbyr en rekke databasetjenester for å hjelpe med velgerregistrering. Disse fullt administrerte systemene kan startes på få minutter med noen få klikk. Videre muliggjør AWS Database Migration Service en enkel og kostnadseffektiv overgang til AWS Cloud.

Slik ble det gjort:

- Det primære registeret med velgerfilinformasjon var en database som var vert på Amazon RDS. Denne databasen kombinerte data fra ulike kilder (inkludert www.barackobama.com og giverinformasjon fra økonomiteamet) for å gi kampanjeledere et dynamisk, fullt integrert bilde av hva som foregikk.
- Denne samlingen av databaser gjorde det mulig for kampanjearbeidere å målrette og segmentere potensielle velgere, skifte markedsføringsressurser basert på tilbakemeldinger i nær sanntid om effektiviteten til spesifikke annonser, og drive et donasjonssystem som samlet inn mer enn 1 milliard dollar (det 30. største netthandelsstedet i verden).

Obama-kampanjens apper tilsvarer i omfang og kompleksitet de som er sett i de største selskapene og datarike oppstart.

For å gi et punkt-for-punkt-eksempel på hvordan valgkampen brukte apper som var tilgjengelige på AWS-skyplattformen og utførte oppgaver både komplekse og massive i skala:

- Vertica og Elastic MapReduce brukes til å modellere enorme mengder data.
- Flerkanals medieadministrasjon via TV, utskrift, online, mobil, radio og e-post med dynamisk produksjon, målretting, retargeting og multivarianttesting, lik det du finner i et kompetent digitalt mediebyrå.
- Koordinering og samarbeid av frivillige, bidragsytere og støttespillere på et sosialt nivå.
- Storskala transaksjonsbehandling.
- Forebygging og beskyttelse av velgermisbruk, inkludert innsamling av hendelser og utplassering av frivillige.
- Et omfattende informasjonsdistribusjonssystem for kampanjenyheter, meningsmålinger, emneinformasjon, velgerregistrering og mer.

Siden det amerikanske presidentvalget i 2016 har Amazon Web Services stille økt sin tilstedeværelse i statlige og lokale valg; mer enn 40 stater bruker nå ett eller flere av Amazons valgtilbud, det samme gjør USAs to store politiske partier, den demokratiske presidentkandidaten Joe Biden, og det føderale byrået som har ansvaret for å håndheve føderale kampanjefinansieringslover.

Selv om det ikke håndterer stemmegivning på valgdagen, ifølge selskapsdokumenter og intervjuer, driver AWS nå statlige og fylkesvalgnettsteder, lagrer velgerregistreringsruller og stemmeseddeldata, letter utenlandsk stemmegivning av militært personell og bidrar til å gi live valgnattresultater.

Ikke desto mindre kan Amazons økende tilstedeværelse i valgindustrien sette det mange tjenestemenn anser som en styrke i det amerikanske valgsystemet: desentralisering.

Mens de fleste sikkerhetseksperter er enige om at mens Amazons sky sannsynligvis vil være mye vanskeligere å hacke enn systemene den erstatter, øker muligheten for at et enkelt stort brudd kan være katastrofalt å sette data fra flere jurisdiksjoner på et enkelt system. "Det gjør Amazon til et mer attraktivt mål for hackere"

og "øker vanskeligheten med å håndtere et innsideangrep," sa Chris Vickery, direktør for cyberrisikoforskning ved cybersecurity-bedriften Upguard.

Privatiseringen av stemmeinfrastruktur er del av en større trend som har feid over nesten alle aspekter av regjeringen i Amerika, fra parkeringsbøter til fengsler, og fortsatte under Trump-administrasjonen.

Ifølge selskaper som samarbeider med begge firmaene for offentlige kontrakter, har Azure, AWS hovedkonkurrent, en betydelig regjeringsvirksomhet og tilbyr noen valgtjenester, men det har ikke fokusert på dem og ligger bak Amazon.

Spørsmål å vurdere:

1. Hva er fordelene med å legge valg på en skyplattform?

2.Hvordan anses desentralisering som en trussel?

3. Les og kommenter hvordan AWS brukte sentimentanalyse til å reflektere over innsettelsestalene til Obama vs Trump og konklusjonene som ble gjort: https://medium.com/@szekelygergoo/use-aws-to-compare-inauguration-speeches-of-obama-and-trump-670068ea39d5

Vedlegg 2: Kodesnutter

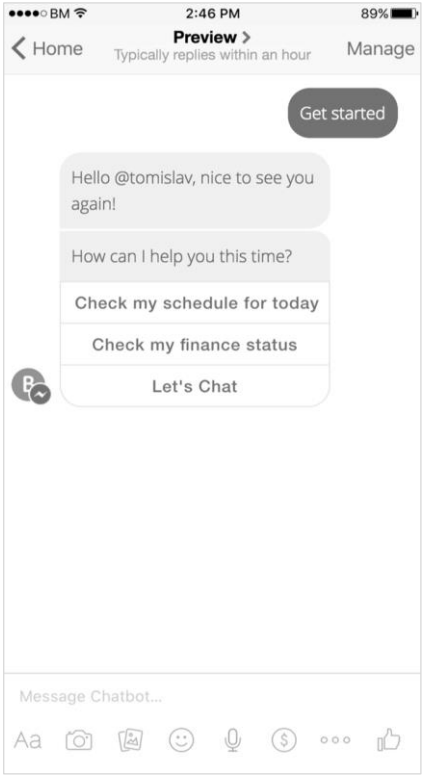
Usecase: Chatbot for studenter i EDU-institusjonen

Viktigheten av naturlig språkforståelse (NLU) kan ikke fremheves nok, men det er hovedgrunnen til at denne avhandlingen i det hele tatt vurderer å bli påmeldt. Fra teknologiperspektiv har Microsoft virkelig god service å tilby. Language Understanding Service (LUIS) er en av de beste NLU-løsningene på markedet. Imidlertid er hver Microsoft-tjeneste som på en eller annen måte er i forhold til NLU, koblet til LUIS i bakgrunnen. Med LUIS er det enkelt å legge til språkforståelse i alle apper. Den er designet for å identifisere verdifull informasjon i samtaler, LUIS tolker brukermål (hensikter) og destillerer verdifull informasjon fra setninger (enheter), for en nyansert språkmodell av høy kvalitet. LUIS integreres sømløst med Azure Bot Service, noe som gjør det enkelt å opprette en sofistikert robot.

```
{
   "query": "Book me a flight to Cairo",
   "topScoringIntent": {
       "intent": "BookFlight",
       "score": 0.9887482
   },
   "intents": [
       {
           "intent": "BookFlight",
           "score": 0.9887482
       },
       {
           "intent": "None",
           "score": 0.04272597
       },
   ],
   "entities": [
       {
           "entity": "cairo",
           "type": "Location",
           "startIndex": 20,
           "endIndex": 24,
           "score": 0.956781447
       }
   ]
}
```


Figur 0.1. LUIS i aksjon

For spørringer som «Bestill en flyreise til Kairo for meg» kan for eksempel LUIS henvende resultatene i et JSON-skjema. hvor man kunne finne verdifull informasjon som BookFlight as an Intent med 98% nøyaktighet og enheter som Kairo som en lokasjonsenhet med 95% nøyaktighet. Selv om Bots og NLU er ganske modne teknologier, er det fortsatt muligheter for at noen spørsmål forblir ubesvart eller misforstått. Disse situasjonene bør behandles godt, og studentene bør ha et annet mulig alternativ for å oppfylle forespørselen. En av vanlige tilnærminger for den situasjonen er raske svar. Hurtigsvar er små knapper eller menyer som allerede har forberedt og forutsagt mulige spørsmål som kan skrives, men også velges ved å trykke på riktig forutsagt spørsmål.



Figur 0.2. Raske svar

En annen mulig løsning er å tilby å chatte eller ringe Student Office Desk Staff direkte, men det bør bare være i sjeldne tilfeller. Hovedidéen med Student Service Support Chatbot er å redusere antall studentsamtaler til et minimum.

Usecase: Sertifisering av digitale eiendeler ved bruk av distribuert journal / blockchain

Applikasjonsmoduler

Denne typen applikasjoner er ment for privat blockchain. Dette betyr at hver utdanningsinstitusjon skal ha sin egen strøm som bare de i institusjonen har myndighet til å lagre vitnemålet. Alle strømmer lagres i hovedboken som distribueres til alle noder, altså utdanningsinstitusjoner i dette eksemplet. Jo flere noder i kjeden, jo bedre, fordi kjeden blir stadig sterkere og tryggere.

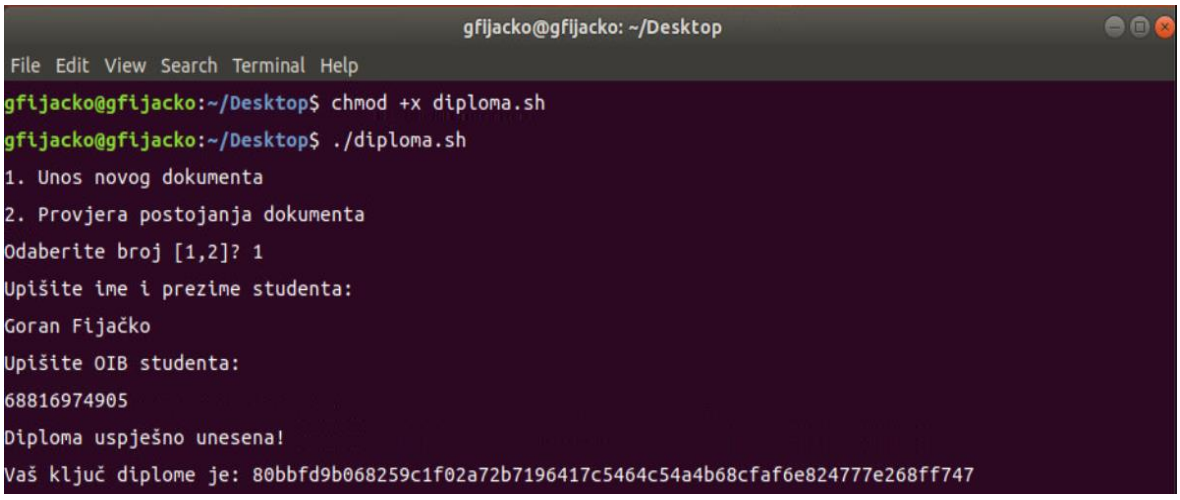
Søknaden består av tre moduler:

1. Modul for å legge inn et diplom
2. Diplom sjekk modul
3. Diplom utskrift modul

Den første modulen er for å legge inn et diplom. Den bytter de angitte dataene til en heksadesimal form og lagrer dem i kjeden og returnerer transaksjons-IDen (txid) tilbake. Transaksjons-ID er en privat nøkkel som tildeles en kandidatstudent fordi den kan brukes til å kontrollere diplomdataene i kjeden. Diploma Check Module, kombinert med OIB og transaksjons-ID, sender en spørring til kjeden og verifiserer om det finnes en post i kjeden. Deretter gir det et positivt eller negativt svar, avhengig av om det er en virkelig nødvendig grad i kjeden og om den er i samsvar med OIB som er inngått. Diplomutskriftsmodulen skriver ut et diplom på skjermen i PDF-format. Alle modulene som er oppført i dette eksemplet, vises i kommandolinjetekstgrensesnittet, dvs. i Ubuntu Operating System Terminal. De kan også programmeres til en webapplikasjon og brukes i nettlesere.

Brukerroller

Etter at studenten har fullført studiet og forsvarer sin hovedfagsoppgave, rapporterer fakultetssystemet at studenten har uteksaminert. Med denne søknaden og modulen for å legge inn diplomet, vil en autorisert person ved universitetet skrive inn navn, etternavn og OIB-kandidatstudent, og denne informasjonen vil bli lagret i kjeden. Som tilbakemelding mottar han en transaksjons-ID som gir studenten og registrerer seg på det originale utskriftsdiplomet. Den kan også skrives ut i form av en strekkode hvis skanning er verdien av transaksjons-ID.



Figur 0.3. Viser modul for oppføring av vitnemål

Studenten får sitt fortjente diplom og sitt private nøkkeldiplom, som i dette tilfellet er 80bbfd9b068259c1f02a72b7196417c5464c54a4b68cfaf6e824777e268ff747. Han rapporterer deretter for en jobb, og etter en samtale fra arbeidsgiveren går han til jobbintervjuet. Arbeidsgiveren ber om en grad for å sjekke kvalifikasjonene hans. Prosedyren gjennomføres for tiden slik at arbeidsgiveren kontakter utdanningsinstitusjonen for å verifisere gyldigheten av vitnemålet, oftest skriftlig. Denne prosessen er langvarig og bruker mye ressurser. Men i dette tilfellet får arbeidsgiveren et diplom med en privat nøkkel.

Arbeidsgiveren utpeker deretter OIB-personen som søker jobb og den offentlige nøkkelen i søknaden. Denne måten på en brøkdel av et sekund returnerer informasjonen om gyldigheten av diplomet.

```
Molim Vas odaberite opciju:
1. Unos novog dokumenta
2. Provjera postojanja dokumenta
Odaberite broj [1,2]? 2
OIB:
68816974905
Ključ:
80bbfd9b068259c1f02a72b7196417c5464c54a4b68cfaf6e824777e268ff747
Goran Fijačko diplomirao na Visokom učilištu Algebra, smjer Multimedija, 15.10.2018. u Zagrebu.
Prikazati diplomu?
1. Da
2. Ne
Odaberite broj [1,2]? 1
Diploma će se prikazati u PDF-u!
```

Figur 0.4. Vis diplombekreftelsesmodulen

Etter at programmets bekreftelse er besvart, skrives skjermen ut. Navnet og etternavnet til studenten, utdanningsinstitusjonen, orienteringen, datoen og stedet for oppgraderingen er skrevet på trykket. Arbeidsgiver har etter hvert mulighet til å skrive ut kopi av vitnemålet til eget arkiv. Hvis du velger et utskriftsalternativ, vil vitnemålet bli generert og åpnet i PDF-format.

For enkel bruk av programmet etter utgivelse til produksjon, er det et bedre valg å bruke det som et WEB-program. Dette betyr at alt som vises vil bli flyttet til en webserver, og applikasjonen vil få tilgang til https-protokollen (f.eks. via URL-https://www.diplome.hr) i nettlesere. Dette betyr at brukerne bare trenger en internettforbindelse og en konto i søknaden for raskt og sikkert å sjekke gyldigheten av vitnemålet.

Usecase: Fjernstyrte smarte enheter i smartbygninger

For å tolke effekten av omgivelsesforholdene i butikkene til kundeatferd kan vi bruke IoT-sensorer til å måle lysstyrke, temperatur og fuktighet og bestemme/kontrollere deres innflytelse på kundenes handlekurver.

Dette innebærer å bestemme terskler for ugunstig lysstyrke, ubehagelig temperatur og utilstrekkelig fuktighetsnivå. Den teknologiske løsningen bør tas i bruk i form av et beslutningsstøttesystem som kan analysere de gjensidige relasjonene mellom IoT-innsamlede data, spesifikke produktgrupper og overordnede transaksjoner i butikken.

En del av beslutningsstøttesystemet skal kunne kontrollere tekniske forhold på automatisert måte gjennom interoperabelt grensesnitt innebygd i eksisterende klimaanlegg. Siden omgivelsesforholdene vanligvis ikke er like i hele butikken fordi noen produkter kan kreve forskjellige forhold (f.eks. har frossen mat et annet akseptabelt omgivelsestemperaturområde enn annen mat), bør vi inkludere butikksonen i analytiske datasett som identifiserer et bestemt område som krever spesifikke miljøforhold.

De foreslåtte datapunktene er delt inn i to granularitetsnivåer: butikkbesøk og kjøpt produkt. Datapunktene hentes fra eksisterende transaksjonsdatabaser og datalageret som inneholder sanntidsdata fra IoT-sensorer.

Transaksjonelle datakildetabeller er som følger i figurene nedenfor.

Miljø

Field Name	Data Type	Description (Optional)
Time	AutoNumber	Time stamp (granulation level is arbitrary)
StoreAreaID	Number	The area of the store
Temperature	Number	Mean temperature of the store area
Brightness	Number	Mean brightness of the store area
Humidity	Number	Mean humidity of the store area

Transaksjoner

Field Name	Data Type	Description (Optional)
VisitID	AutoNumber	
ProductID	Short Text	Bought product during the visit
Quantity	Number	Quantity of the bought product

StoreAreas

Field Name	Data Type	Description (Optional)
StoreAreaID	AutoNumber	
StoreAreaName	Short Text	The name of the area of the store

Produkter

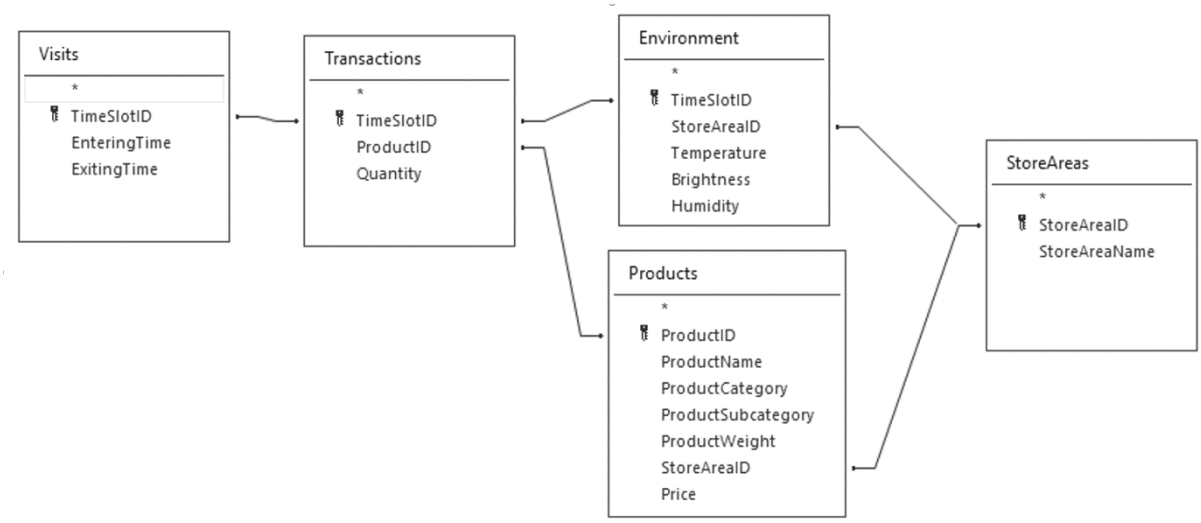
Field Name	Data Type	Description (Optional)
ProductID	AutoNumber	
ProductName	Short Text	The name of the product
ProductCategory	Short Text	The category of the product
ProductSubcategory	Short Text	The subcategory of the product
ProductWeight	Number	The weight of the one unit of the product
StoreAreaID	Short Text	The area in which the product is located in the store
Price	Number	Price of one unit of the product

Besøk

Field Name	Data Type	Description (Optional)
VisitID	AutoNumber	
EnteringTime	Date/Time	Time when customer entered the store
ExitingTime	Date/Time	Time when customer arrived to the cash register

Figur 0.4. Transnasjonal datakilde

På figuren nedenfor er ETL-relasjonene vist:



Figur 0.5. ETL-relasjoner

Variablene som er tilgjengelige for å analysere butikkbesøk etter bruk av ETL-prosedyre er:

Field Name	Data Type	Description (Optional)
TimeSlotID	AutoNumber	
EnteringTime	Date/Time	
ExitingTime	Date/Time	
ProductID	Number	
Quantity	Number	
Environment_StoreAreaID	Number	
Temperature	Number	
Brightness	Number	
Humidity	Number	
ProductName	Short Text	
ProductCategory	Short Text	
ProductSubcategory	Short Text	
ProductWeight	Number	
Products_StoreAreaID	Number	
Price	Number	
StoreAreaName	Short Text	

Figur 0.6. Variablene etter bruk av ETL-prosedyre

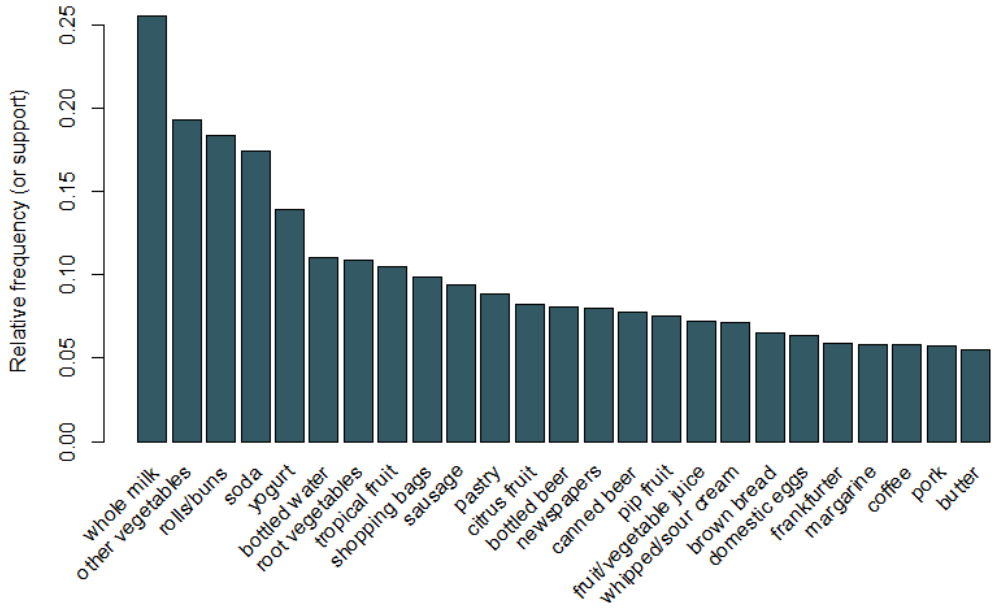
Som målvariabler for maskinlæring kan vi nå utlede:

- Antall varer (N) – antall forskjellige produkter kjøpt av en kunde under ett butikkbesøk (dvs. antall varer i handlekurven);
- Vekt på kjøp (W) – vekt på alle produkter kjøpt av en kunde under ett butikkbesøk
- Antall varer (Q) - antall varer av alle produkter (summert på tvers av alle typer produkter) kjøpt av en kunde i ett butikkbesøk.

Andre grupper av mulige målvariabler – detaljhandelsindikatorer – er beskrevet separat i neste avsnitt.

Usecase: Automatisering av oppgaver ved hjelp av skybaserte tjenester

For å demonstrere hvordan man utfører et Market Basket Analysis ble programmeringsspråket R brukt, og spesielt arules-pakken, sammen med noen kode inkludert som et proof-of-concept. Eksemplet som brukes er tilgjengelig på arulesViz Vignette og bruker et datasett med dagligvaresalg som inneholder 9 835 individuelle transaksjoner med 169 varer. Første skritt var å se på postene i transaksjonene og spesielt plotte den relative frekvensen av de 25 hyppigste postene. Dette tilsvarer støtten for disse elementene, der hvert varesett bare inneholder enkeltvaren. Barplottet i figur 5.8. illustrerer dagligvarene som ofte kjøpes i denne butikken, og det er bemerkelsesverdig at støtten til selv de hyppigste varene er relativt lav (for eksempel forekommer den hyppigste varen i bare rundt 2,5% av transaksjonene). Denne innsikten ble brukt til å informere minimumsterskelen når du kjører Apriori-algoritmen; For eksempel vet vi at for at algoritmen skal returnere et rimelig antall regler, må vi sette støtteterskelen til godt under 0,025.



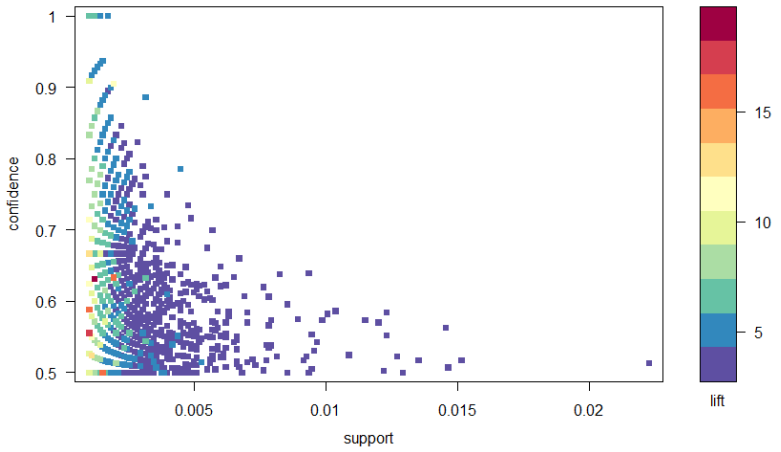
Figur 0.7. Bar plot av støtten til de 25 hyppigste varene som er kjøpt

Ved å sette en støtteterskel på 0,001 og konfidensen på 0,5, kan vi kjøre Apriori-algoritmen og få et sett med 5 668 resultater. Disse terskelverdiene er valgt slik at antall regler som returneres er høyt, men dette tallet ville reduseres hvis vi økte enten terskel eller støtte. Det anbefales å eksperimentere med disse tersklene for å oppnå de mest passende verdiene. Selv om det er for mange regler til å kunne se på alle individuelt, kan vi se på de fem reglene med størst økning i tabell 5.1 nedenfor.

Tabell 0.1. De fem reglene med størst løft

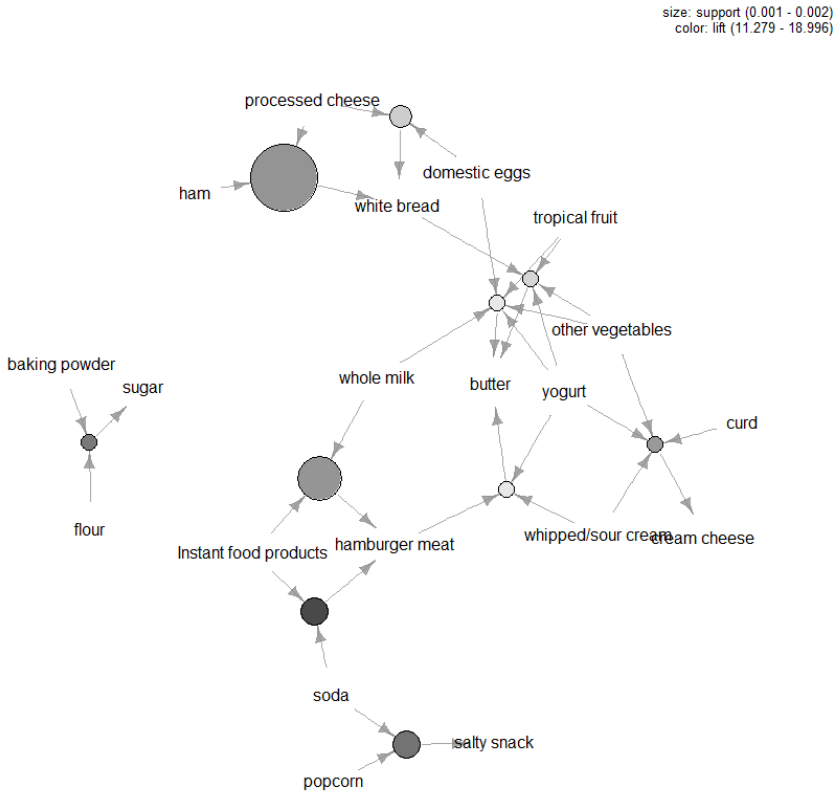
Regel	Støtte	Tillit	Løft
{instant matvarer, brus}=>{hamburgerkjøtt}	0.001	0.632	19.00
{brus, popcorn}=>{salt snacks}	0.001	0.632	16.70
{mel, bakepulver}=>{sukker}	0.001	0.556	16.41
{skinke, bearbeidet ost}=>{hvitt brød}	0.002	0.633	15.05
{helmelk, instant matvarer}=>{hamburgerkjøtt}	0.002	0.500	15.04

Disse reglene ser ut til å gi intuitiv mening. Den første regelen kan for eksempel representere den typen varer som er kjøpt for en grillfest, den andre for en filmkveld og den tredje for baking. I stedet for å bruke tersklene til å redusere reglene ned til et mindre sett, er det vanlig at et større sett med regler returneres slik at det er større sjanse for å generere relevante regler. Alternativt kan vi bruke visualiseringsteknikker for å inspisere settet med regler som returneres og identifisere de som sannsynligvis vil være nyttige. Ved hjelp av ***arulesViz-pakken*** plottes regler for tillit, støtte og løft. Dette plottet, vist i figur 5.9., illustrerer forholdet mellom de ulike beregningene. De optimale reglene er de som ligger på det som kalles «støtte-tillitsgrense». I hovedsak ligger de på høyre kant av tomten der enten støtte, tillit eller begge deler er maksimert. Plottfunksjonen i *arulesViz-pakken* har en nyttig interaktiv funksjon som lar deg velge individuelle regler (ved å klikke på det tilhørende datapunktet), noe som betyr at reglene på grensen lett kan identifiseres.



Figur 0.8. Et spredt diagram over beregningene for tillit, støtte og økning

Det er mange andre diagrammer tilgjengelig for å visualisere reglene, men en annen figur som vi vil anbefale å utforske er grafbasert visualisering av de ti beste reglene når det gjelder løft (mer enn ti regler kan inkluderes, men denne typen grafer kan lett bli rotete). I figur 5.10. representerer elementene som er gruppert rundt en sirkel, et elementsett, og pilene angir relasjonen i regler. For eksempel er kjøp av sukker forbundet med kjøp av mel og bakepulver. Størrelsen på sirkelen representerer konfidensnivået som er knyttet til regelen, og fargen løftenivået (jo større sirkelen og jo mørkere grå, jo bedre).



Figur 0.9. Grafbasert visualisering av de ti beste reglene når det gjelder økning

Market Basket Analysis er et nyttig verktøy for forhandlere som ønsker å bedre forstå forholdet mellom produktene som folk kjøper. Det er mange verktøy som kan brukes når du utfører MBA, og de vanskeligste aspektene ved analysen er å sette tillits- og støttetersklene i Apriori-algoritmen og identifisere hvilke regler som er verdt å forfølge. Vanligvis gjøres sistnevnte ved å måle reglene i form av beregninger som oppsummerer hvor interessante de er, ved hjelp av visualiseringsteknikker og også mer formell multivariat statistikk.

Til syvende og sist er nøkkelen til MBA å trekke ut verdi fra transaksjonsdataene dine ved å bygge opp en forståelse av forbrukernes behov. Denne typen informasjon er uvurderlig hvis du er interessert i markedsføringsaktiviteter som kryssalg eller målrettede kampanjer.

R-kode

```
bibliotek("regler")

bibliotek ("arulesViz")

 #Load datasett:

data("Dagligvarer")

sammendrag(Dagligvarer)

#Look på data:

inspisere (dagligvarer [1])

LISTE (Dagligvarer)[1]

 #Calculate regler ved hjelp av apriori-algoritmen og spesifisering av støtte- og konfidensterskler:

regler = apriori(Dagligvarer, parameter=liste(support=0.001, confidence=0.5))

#Inspect de 5 beste reglene når det gjelder løft:

inspisere(overhode(sortere(regler, ved ="løft");5))

#Plot et frekvensplott:

itemFrequencyPlot(Dagligvarer, topN = 25)

 #Scatter handlingen av regler:

bibliotek ("RColorBrewer")

plott(regler;kontroll=liste(col=brewer.pal(11,"spektral")),main="")

#Rules med høyt løft har vanligvis lav støtte.

#The mest interessante reglene ligger på støtte/tillitsgrensen som tydelig kan sees i dette plottet.

 #Plot grafbasert visualisering:

underregler2 <- hode(sorter(regler; by="løft"), 10)
```

plott **(underregler2, metode** = "graf",kontroll = liste (type = "elementer",hoved = ""**))**

Usecase: Vannforsyningsstyring ved hjelp av avstandslesere i vannforsyningsnett

LoRa-protokollen er en modulering av trådløs dataoverføring basert på eksisterende Chirp Spread Spectrum (CSS) -teknologi. Med sine egenskaper tilhører den gruppen av protokoller med lavt strømforbruk og stort dekningsområde (LPWAN). Når man ser på OSI-modellen, tilhører den det første, fysiske laget. Historien til LoRa -protokollen begynner med det franske selskapet Cycleo, hvis grunnleggere opprettet et nytt fysisk lag med radiooverføring basert på den eksisterende CSS-modulasjonen. Målet deres var å tilby trådløs datautveksling for vannmålere, strøm- og gassmålere. I 2012 kjøpte Semtech Cycleo og utviklet brikker for klient- og tilgangsenheter. Selv om CSS-modulering hittil hadde blitt brukt på militære radarer og satellittkommunikasjon, LoRa hadde forenklet applikasjonen, eliminere behovet for presis synkronisering, med introduksjonen av en veldig enkel måte å kode og dekode signaler på. På denne måten ble prisen på sjetonger akseptabel for utbredt bruk. LoRa bruker ulisensiert frekvensspektrum for sitt arbeid, noe som betyr at bruken ikke krever godkjenning eller leie av konsesjon fra regulatoren. Disse to faktorene, lave kostnader og gratis bruk, har gjort denne protokollen ekstremt populær på kort tid.

EBYTE E32 (868T20D)-modulen ble brukt til å opprette prosjektet. Modulen er basert på Semtech SX1276-brikken. Modulens maksimale utgangseffekt er 100 mW, og produsenten har erklært en rekkevidde på opptil 3 km ved hjelp av en 5dBi-antenne uten hindringer, med en overføringshastighet på 2,4 kbps. Denne modulen har ikke en integrert LoRaWAN-protokoll, men er designet for direkte kommunikasjon (P2P). Hvis den skal brukes til LoRaWAN, da protokollen må implementeres på en mikrokontroller. Kommunikasjon mellom modulen og mikrokontrolleren realiseres gjennom UART-grensesnittet (seriell port) og to kontrollterminaler, som brukes til å bestemme modulens driftstilstand. Modulen vil returnere tilbakemelding via AUX-setningen.

LoRaWAN er en programvareprotokoll basert på LoRa -protokollen. I motsetning til den patentbundne LoRa -overføringsprotokollen, LoRaWAN er en åpen industristandard som drives av den ideelle organisasjonen LoRa Alliance. Protokollen bruker et ulisensiert ISM-område (industri, vitenskap og medisin) for sitt arbeid. I Europa, LoRaWAN bruker ISM-delen av spekteret som dekker området mellom 863 - 870 MHz [4]. Dette området er delt inn i 15 kanaler med forskjellige bredder. For at en enhet skal være LoRaWAN-kompatibel, den må kunne bruke minst de fem første kanalene på 125 kHz og støtte overføringshastigheter på 0.3 til 5 kbps. På grunn av beskyttelsen mot frekvensbelastning, driftssyklusen til LoRaWAN-enheten er veldig lav og overføringstiden må ikke overstige 1% av enhetens totale drift.

I tillegg til å definere typen enheter og måten de kommuniserer via meldinger, LoRaWAN-protokollen definerer også utseendet til selve nettverket [5]. Den består av sluttenheter, vanligvis forskjellige typer sensorer i kombinasjon med LoRaWAN-enheter. Sensorene vises til sentrale transceivere eller konsentratorer. Én sensor kan reagere på flere huber, noe som forbedrer nettverkets motstandskraft og rekkevidde. Huber er koblet sammen med servere som behandler innkommende meldinger. En av oppgavene til serveren er å

gjenkjenne flere mottatte meldinger og fjerne dem. Sentrale transceivere må kunne motta et stort antall meldinger ved hjelp av flerkanals radiotransceivere og adaptiv modus, og tilpasse seg funksjonene til sluttenheten. Sikkerheten til LoRaWAN-nettverket sikres ved å autorisere sensoren til den sentrale transceiveren, og meldinger kan krypteres mellom sensoren og applikasjonsserveren via AES-kryptering.

MQTT er en enkel meldingsprotokoll. Den ligger i applikasjonslaget til TCP / IP-modellen (5-7 OSI-modeller). Den ble opprinnelig designet for meldinger i M2M-systemer (direktemeldinger mellom maskiner). Den største fordelen er det lille behovet for nettverks- og dataressurser. Av disse grunnene, det har blitt en av de viktigste protokollene i IoT-verdenen. Denne protokollen er basert på prinsippet om abonnement på meldinger og publisering av dem gjennom mellommenn. En mellommann, ofte kalt en megler, er en server som mottar og distribuerer meldinger til klienter som kan være utgivere av meldinger eller kan abonnere på dem for å motta dem. De to klientene vil aldri kommunisere med hverandre.

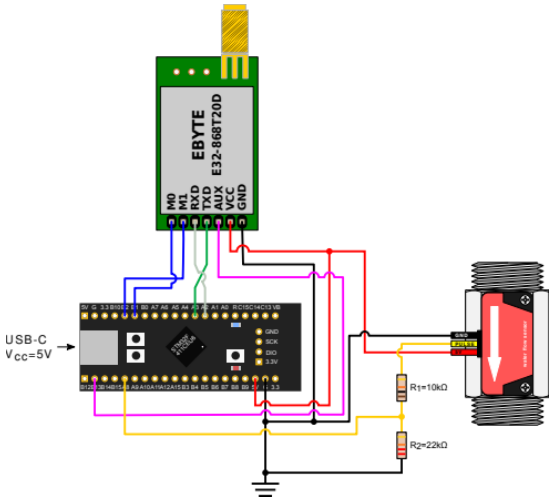
Det viktigste segmentet av sensorplattformen er påliteligheten. For å sikre at en ulykke skjer i tide, må vi først sikre påliteligheten til plattformen. Nettopp av denne grunn, i løsningen foreslått i dette skrivet, er periodisk rapportering fra sensorplattformen til systemet satt. Enheten vil rapportere med jevne mellomrom hver 12. time, og dette ivaretas av alarmsystemet på mikrokontrolleren. STM32F411 er nemlig utstyrt med en klokke som overvåker sanntid (RTC), og tilbyr muligheten til å stille inn to uavhengige alarmer. I dette tilfellet har en av dem ansvaret for å vekke prosessen som sender periodiske meldinger med gjeldende tilstand for den målte vannstrømmen gjennom måleren.

Før programvareimplementeringen av målingen, bør det bemerkes at pulsen gitt av sensoren ved utgangsspenningen er 5 V. Selv om den brukte mikrokontrolleren vil tolerere denne spenningen ved inngangen, er det bedre å senke den til den deklarerte inngangsverdien på 3,3 V. Slik spenning oppnås med to motstander, en med en verdi på 10 kΩ og den andre på 22 kΩ, koblet i en enkel spenningsdeler [9]. Tilkoblingsmetoden er tydelig vist i diagrammet. Selve mengdemålingen gjøres ved å overvåke antall pulser som sendes av vannsensoren via en standard tidsteller. Hver puls vil bli registrert av mikrokontrolleren som et avbrudd. Når pulser vises, det er mulig å måle strømmen og rapportere den via LoRa radiooverføring.

Frekvensen til timeren er satt til 1 MHz via en skillelinje. Ved å sammenligne antall klokkesykluser mellom de to avbruddene, kan man veldig enkelt få pulsfrekvensen gitt av vannstrømningssensoren. Å vite pulsfrekvensen og pulskarakteristikken, kan vannstrømmen beregnes ved hjelp av forhåndsdefinert prosedyre. Se figur 5.11. for tilkoblinsskjema for en vannstrømmingssensor.

Den første målte strømningsverdien større enn null setter sensorplattformen til alarmtilstand. Så lenge det er en flyt, vil periodisk annonsering finne sted hvert 15. minutt i stedet for hver 12. Fem minutter etter at strømmen stopper, vil enheten høres slutten av alarmen, og neste samtale vil bli foretatt regelmessig etter 12 timer eller tidligere i tilfelle en ny alarm. Alarmsystemet fungerer internt på en slik måte at den siste målte verdien av vannstrømmen leses av hvert 5. Denne verdien, sammen med gjeldende tellertid, lagres kontinuerlig av måleprosessen i form av en tids- og strømningsstruktur. Leseverdien lagres i et felt på størrelse

med tre elementer. Hvis alle tre elementene i feltet etter tre avlesninger er like, kan det bestemmes at det ikke var strøm de siste 15 sekundene, og enheten avslutter alarmtilstanden. Systemet venter ytterligere fem minutter før det kunngjør slutten på alarmen over LoRa-tilkoblingen. Hvis strømmen skjer igjen i løpet av disse fem minuttene, vil systemet fungere som om alarmen ikke har stoppet, det vil si at det vil sende en flytmelding etter 15 minutter.



Figur 0.10. Tilkoblingsskjema for vannstrømningssensor

LoRa -varsler er med vilje forsinket slik at i tilfelle en konstant forekomst og avbrudd i strømmen, de vil ikke ofte sende radiomeldinger.

Erfaringer fra virkeligheten

Under målingen leveres kretsen med 5 V DC. Dette er den anbefalte driftsspenningen for LoRa-modulen og vannstrømningssensoren som brukes, mens mikrokontrolleren kan drives av 5 V eller 3.3 V. I denne målingen er det første målet å vise at toppstrømverdien ikke vil nå en verdi større enn 300 mA, som er det maksimale mikrokontrollerkretsen tåler. Disse dataene lar oss drive hele kretsen gjennom mikrokontrolleren ved hjelp av den innebygde USB-porten og dermed forenkle utseendet til hele sensoren. Det andre målet er å redusere strømforbruket for å forlenge autonomien til sensoroperasjonen så mye som mulig. Som ekstern strømforsyning ble det brukt en laboratoriestrømforsyning R-SPS3010 fra Nice-power, som kan gi en stabil driftsspenning fra 0 til 30 V med en strøm på opptil 10 A. Det universelle måleinstrumentet UT139B fra UNI-T er seriekoblet. Den er satt til å måle milliampere under målingen, og holder den maksimale målte verdien på skjermen.

Måling av rekkevidde

Rekkevidden ble målt fra Zagreb-bosetningen Vrbani 3, som ligger ved siden av Jarunsjøen. Denne beliggenheten gir oss et innblikk i hvilken rekkevidde som kan forventes i urbane og hva i landlige forhold. Nemlig, fra den sentrale transceiveren i nord er det en veldig urban del med mange boligbygg og tett trafikkinfrastruktur, mens på sørsiden er Lake Jarun og Sava-elven, som for det meste er grønne områder, mindre skoger og bare noen få lavere bygninger. Den begrensende faktoren er posisjonen til antennen til den sentrale transceiveren, som befant seg i første etasje i en boligbygging, ca 4 m over bakkenivå og omgitt av bygninger. Ved måling på siden av sentraltransceiveren ble det brukt en omnidireksjonell antenne med en forsterkning på 3, 5 dBi, som er stasjonær plassert på utsiden av vinduet i en boligbygging. På sensorsiden, for mobilitet, ble det brukt en mindre antenne med 2 dBi-forsterkning. Signalet ble sendt i det åpne "ut av hånden". Posisjonen til hver måling ble registrert via en GPS-enhet på en mobil enhet og senere overført til Google Earth. I Google Earth er det mulig å importere registrerte målepunkter og måle avstanden mellom dem og antennen til den sentrale transceiveren. I henhold til produsentens spesifikasjoner er den maksimale rekkevidden som kan forventes fra disse modulene 3 km under nesten ideelle forhold med en 5 dBi-antenne. For på en eller annen måte å nærme seg denne avstanden til tross for den ugunstige måleposisjonen, ble dataoverføringshastigheten redusert fra standardmodulinnstillingene fra 2, 4 kbps til 300 bps. På grunn av den lille mengden data som må overføres, er dette ikke en begrensende faktor i praksis, og på grunn av den lave overføringshastigheten ble det oppnådd en mindre mengde feil ved gjenkjenning av det mottatte signalet og økt suksess med å motta meldinger over lange avstander. I figuren under det målte området til det fabrikkerte LoRa-systemet vises. Posisjonen til den sentrale transceiveren vises med en stjerne, mens punktene som signalet fra sensoren klarte å nå det, vises i grønt. Røde prikker indikerer steder der det ikke var mulig å kommunisere mellom sensoren og den sentrale transceiveren. Som forventet ble den største rekkevidden på 3393 m oppnådd i sørøst, hvor bortsett fra et par boligbygg i nærheten av antennen, var det ingen ekstra hindringer. Mot sørvest var det oppnådde resultatet 2773 moh. Men ifølge den urbane delen av byen var maksimal oppnådd rekkevidde 982 m mot øst, og i nord var det bare 860 m.

Figur 0.11. Sentral transceiverantenneposisjon og måleområde

I henhold til spesifikasjonen er det maksimale forbruket av den brukte modulen 130 mA. Det målte forbruket til vannstrømningssensoren er 4 mA. Maksimal strøm som kan ledes gjennom utviklingskortet for sensorkortet

er 300 mA, og kretsen på utviklingsplattformen som brukes er utformet slik at Vbus USB-terminalen og 5 V-terminalene til kretsen er på samme buss. Fra dette kan vi konkludere med at hele grensesnittet med sensoren og LoRa-modulen kan drives av USB-grensesnittet. Det er imidlertid nødvendig å optimalisere forbruket slik at kretsen kan kjøre på et kommersielt tilgjengelig batteri så lenge som mulig. Tabell viser gjeldende målinger under drift av mikrokontrolleren. Her opererte mikrokontrolleren med en maksimal driftsklokke på 96 MHz og uten strømoptimalisering. Data gis separat for hvert element for å gjøre det enklere å spore optimalisering.

Tabell 0.2. Kretsstrøm uten optimalisering

Tilkoblede systemkomponenter	Gjeldende [mA]	Tilstand
Mikrokontroller	26.65	Vent
Mikrokontroller	26.88	Hendelsestopp
Mikrokontroller + LoRa-modul	39.16	Vent
Mikrokontroller + LoRa-modul	121.5	Send signal
Mikrokontroller + LoRa-modul + sensor	42.51	Vent
Mikrokontroller + LoRa-modul + sensor	125.7	Send signal

Siden strømningssensoren ikke har mulighet for optimalisering, blir verdiene av strømmen som strømmer gjennom den i tabell utpekt, og på slutten av hvert trinn vil de bare bli lagt til de oppnådde resultatene. Tabellen viser at ved å redusere driftsklokken, reduserte strømmen med 11 mA, noe som er en reduksjon på litt mer enn 40% i forbruket av mikroprosessorer.

Tabell 0.3. Strøm gjennom vannsensoren

Gjeldende [mA]	Tilstand
3.35	Uvirksom
4.03	Flyt

Det første trinnet med optimalisering er å senke prosessorklokken til 48 MHz.

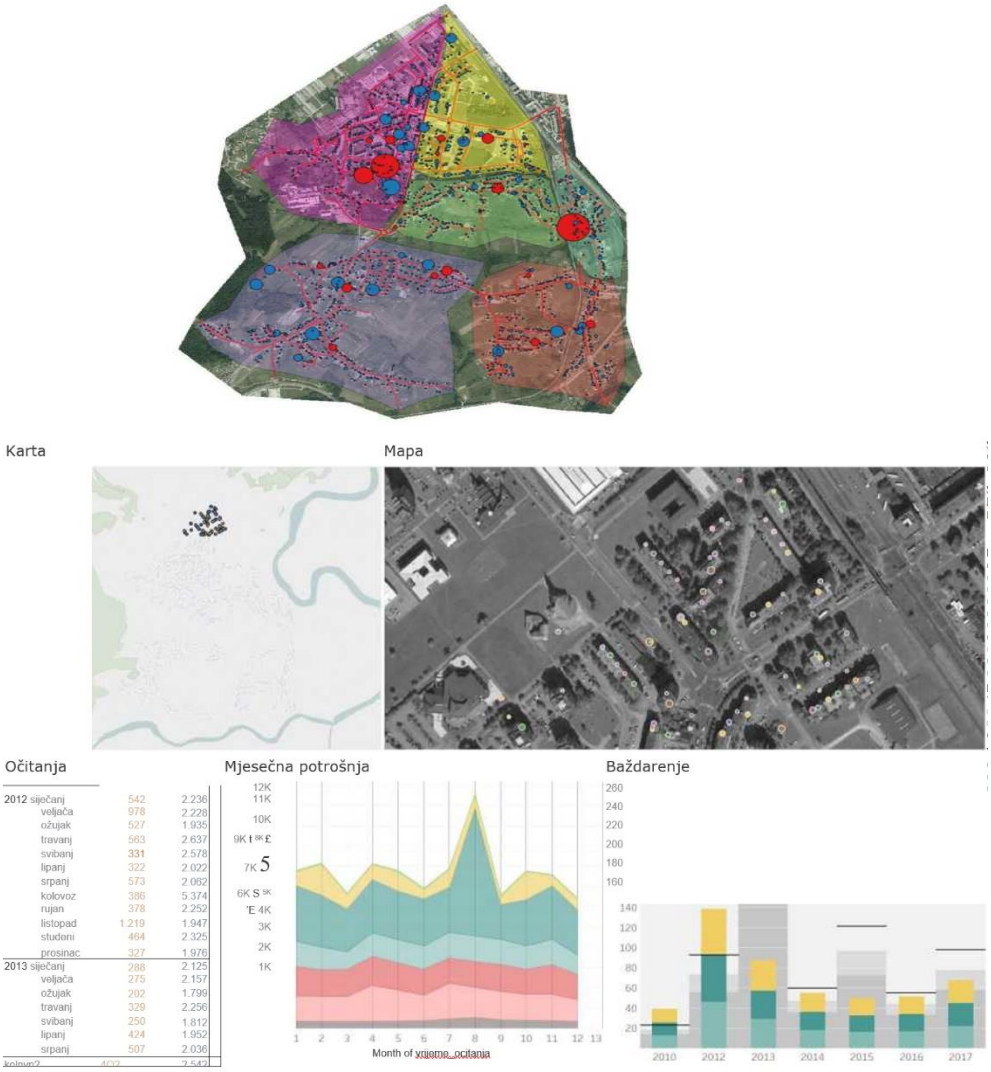
Tabell 0.4 Strøm med redusert mikroprosessorklokkehastighet

Tilkoblede systemkomponenter	Gjeldende [mA]	Tilstand
Mikrokontroller	15.50	Vent
Mikrokontroller	15.91	Hendelsestopp
Mikrokontroller + LoRa-modul	28.15	Vent

Siden LoRa-modulen på sensorplattformen ikke brukes til å motta meldinger, det er ikke nødvendig å holde den konstant aktiv. Heldigvis har denne modulen en modus der den slår av radiosenderen. Ved å endre koden på mikrokontrolleren ble det innført en driftsmodus der radiotransceiveren bare slås på når det er nødvendig. Med denne prosedyren, den totale strømmen gjennom mikrokontrolleren og LoRa-modulen falt til 17.7 mA i standby-modus. STM32F411 mikrokontroller har forskjellige energisparefunksjoner. En av dem er en hvilemodus der vi stopper prosessorklokken helt og bare lytter til forstyrrelser som kommer fra eksterne enheter eller klokker. Siden FreeRTOS ble brukt i skrivet, i stedet for å sende mikroprosessoren direkte i dvale, ble FreeRTOS tickless-modus brukt. I den slutter FreeRTOS å fungere og setter mikroprosessoren i dvale. Dette senker strømmen gjennom kretsen som består av mikrokontrolleren og LoRa-modulen til 5.87 mA i standby-modus, med den totale strømmen gjennom hele kretsen nå bare 9.22 mA i standby-modus.

Måling av strømstyrken har vist hvordan det er mulig å bruke en USB-port til å drive hele kretsen. Også i flere inngrep på programkoden til mikroprosessoren var det mulig å senke strømmen fra 42, 51 mA til 9, 22 mA, noe som er en forskjell på 78%. Dette er veldig viktig fordi ventetid er tilstanden der kretsen ligger nesten hele tiden. Ved hjelp av en bærbar USB-lader (strømbank) med en kapasitet på 10000 mAh (den vanligste verdien i skrivende stund), kan slikt forbruk regnes med omtrent 40 dager med autonom drift av sensoren.

Radiosignalinnsamling viste svært gode resultater med tanke på antennens kraft og posisjon. Denne målingen er en indikasjon på hvordan selv uten et stort søk etter den ideelle antenneposisjonen, kan et ganske anstendig område oppnås med en enhet som har utgangseffekten til et gjennomsnittlig Wi-Fi-hjemmesystem. Maksimal målt avstand var 3393 m målt fra bakkenivå og uten optisk sikt. Det er også en stor forskjell i oppførselen til LoRa -radioprotokoller mellom urbane og landlige områder. Mens rekkevidden i et ubebodd område overgikk produsentens spesifikasjoner, falt rekkevidden kraftig på steder med flere boligbygg. Det kan konkluderes med at for å rapportere bivirkninger i landlige og avsidesliggende områder, LoRa LPWAN er en utmerket løsning. Mindre rekkevidde i byområdet er veldig enkelt å kompensere med tettere plasserte sentrale transceivere.



Figur 0.12. LoRa LPWAN

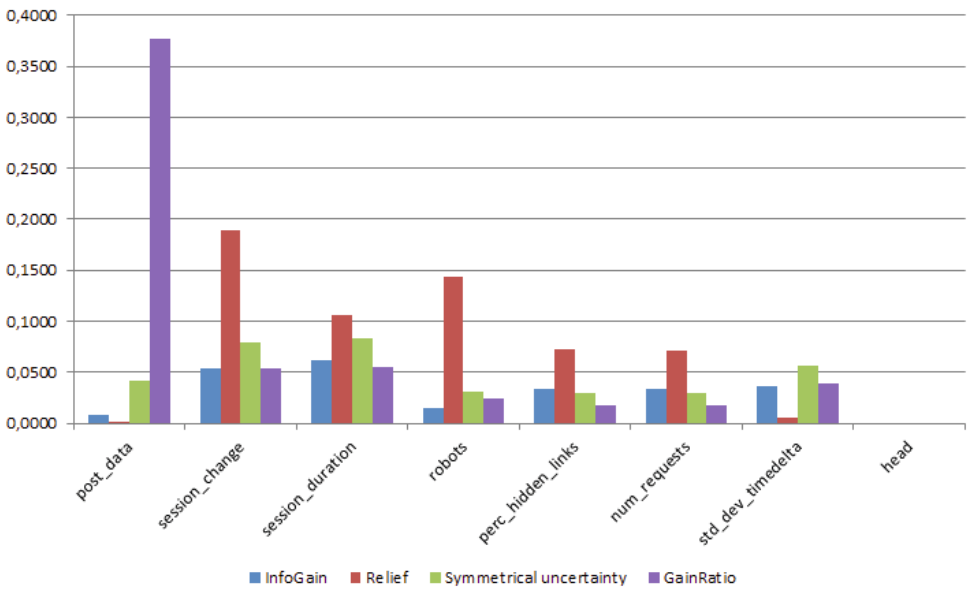
Brukertilfelle: Regelbasert klassifisering av phishing-nettsteder

Før treningen av klassifiseringsmodellen, var det nødvendig å velge funksjonene som er relevante og nyttige for klassifiseringsprosessen. For å evaluere funksjonene brukte vi rangeringen av funksjoner basert på følgende metoder:

- Informasjonsgevinst som rangerer funksjoner basert på den beregnede informasjonsgevinsten i forhold til klassifiseringsklassen, blir numeriske trekk først diskretisert.
- Forsterkningsgrad rangerer funksjoner basert på det beregnede gevinstforholdet. Forsterkningsgrad beregnes som informasjonsgevinst dividert med entropien til funksjonen som forholdet beregnes for.
- Symmetrisk usikkerhet er et mål som eliminerer overflødige og meningsløse funksjoner, som ikke har sammenkobling med andre funksjoner.

- Relief-metoden ble foreslått av Kira og Rendell og brukes til valg av statistisk relevante funksjoner, den er motstandsdyktig mot støy i dana og gjensidig avhengighet av funksjoner.

Funksjoner evalueres på en måte som er tilfeldig samplet fra et gitt sett med forekomster og tar nærmeste naboer som tilhører klassen. Hvis naboene er på linje med forekomster, øker vektingsfaktoren, men hvis de nærmeste naboene er forskjellige, reduseres vektingsfaktoren.



Figur 0.13. Sammenligning av ulike metoder for funksjonsvalg

Hvis vi ser på de rangerte funksjonene i figur 5.14., ser vi at funksjonene som dominerer datasettet er:

- postdata, som viser oss om klienten har fylt ut / ikke fylt ut falsken
- skjema i Lino-systemet
- øktendring, som viser oss om brukeren i løpet av økten har endret
- øktidentifikator eller ikke
- Øktens varighet, varigheten av økten i sekunder
- roboter, som viser oss om brukeren fikk tilgang til / ikke fikk tilgang til roboter.txt fil, som definerer reglene for robotadferd.

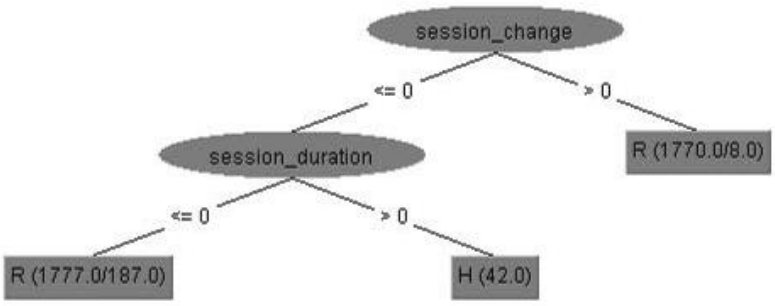
De nevnte funksjonene ble valgt manuelt, vi rangerte alle funksjoner i henhold til poengsummen til funksjonsvalgmetoden. Vi valgte de viktigste funksjonene for klassifiseringsmodellene våre, i vårt tilfelle de fem beste funksjonene.

Valg av klassifiseringsmodell for roboter fra menneskelig differensiering

En forutsetning for å bruke veiledede læringsmetoder og velge det optimale delsettet av funksjoner er et merket datasett. Utvalgte funksjoner skal bidra til generalisering av noen klasser, dvs. For hver klasse skal de kunne lage en unik atferdsprofil. For å evaluere ytelsen til klassifiseringsmetoden brukte vi K-fold kryssvalideringsmetoden. For vårt formål brukte vi k = 10 deler - relevant litteratur sier at k = 10 deler er et optimalt tall for estimering av feil.

Beslutningstreet C 4.5

For det første, for klassifiseringsformål, evaluerte vi en algoritme for beslutningstre C 4.5 (figur 5.15.), som er en oppgradering av den klassiske algoritmen ID3. Begge algoritmene er resultatet av forskning gjort av Ross Quinlan. C 4.5 bruker et datasett for å lære å lage et overflødig tre. Ved bruk av lignende data, i læring og validering.



Figur 0.14. Beskåret tre, ved hjelp av hele settet med funksjoner

Klassifiseringen har gode resultater, men når vi bruker et uavhengig valideringssett, gir klassifisereren vanligvis dårlige resultater. Etter å ha bygget et overflødig tre, konverteres treet til IF/THEN-reglene, og algoritmen beregner de beste betingelsene for klassifiseringsnøyaktighet, vi fjerner HVIS-betingelsene hvis de ikke reduserer klassifiseringsnøyaktigheten. Beskjæring gjøres fra bladene til roten av treet og er basert på den pessimistiske estimeringen av feil; Feil er relatert til prosentandelen av feil klassifiserte tilfeller i treningsdatasettet. Basert på forskjellen i nøyaktighet av regler og standardavvik hentet fra binomialfordelingen, definerer vi en viss øvre konfidensgrense som vanligvis er 0,25, basert på hvilken trærne beskjæres. For å bygge modellene våre med C 4.5 setter vi konfidensterskelen for beskjæring til 0.25 og minimum antall forekomster per blad er 2.

	Class	TP Rate	FP Rate	F-measure	AUC
C 4.5 Experiment #1	Human	0.177	0	0.301	0.773
	Robot	1	0.823	0.972	0.773
C 4.5 Experiment #2	Human	0.793	0.002	0.872	0.985
	Robot	0.998	0.207	0.992	0.985
SVM Experiment #1	Human	0.265	0	0.419	0.801
	Robot	1	0.735	0.979	0.801
SVM Experiment #2	Human	0.962	0.006	0.942	0.976
	Robot	0.998	0.042	0.997	0.978

Figur 0.15. Klassifiseringsresultater for C 4.5 og SVM, eksperiment 1 bruker bare utvalgte funksjoner. Eksperiment 2 bruker utvalgte funksjoner pluss klientens land og forhåndsvarsel

Før klassifiseringen fjernet vi klasseforekomsten av ukjente besøkende fordi de representerte menneskelige forsøk på å angripe med manuelt angitte valer eller ved hjelp av ikke-eksisterende nettlesere. Metode C 4.5 har resultert i at det beskårne treet vises, noe som er det samme med det optimale utvalget av funksjoner og bruk av hele settet med funksjoner. Det er viktig å merke seg at algoritmen C 4.5 er veldig god til å velge funksjoner ved å bruke heuristikk ved å opprette og slette undertrær.

Hvis vi ser på resultatene i figur 5.16., kan vi se at for de gitte funksjonene (eksperiment 1) har vi en klassifiseringsnøyaktighet på 94.5% og en perfekt frekvens av riktige positive for roboter (TP-rate). Klassifisereren klassifiserer dårlig menneskelige besøkende (TPR = 0, 177), og forringer klassifiseringsevnen til roboten der frekvensen er falsk positiv rate er høy - 0, 823. Ser vi på F-mål, kan vi si at en god klassifiserer oppdager korrekt roboter mens feilaktig klassifiserer menneskelige besøkende og ofte (> 80%) erklærer dem roboter. Vi testet C 4.5 classier med to tilleggsfunksjoner - kundens land og ASN av tjenesteleverandøren. Disse funksjonene ble løst fra IP-adressen ved hjelp av den nevnte GeoIP-databasen. Denne delmengden (C 4.5 eksperiment 2) er vist i tabell. Vi reduserte antall falske positiver for klassen Robot til 0.207, slik at resultatet av klassifisering for klasse Human var bedre 0.793.

Støtte vektormaskin

SVM er en algoritme som finner den maksimale separasjonsmarginen mellom klasser, mens den definerer marginen som avstand mellom de kritiske punktene som er nærmest separasjonsoverflaten. Punkter nærmest overflaten kalles støttevektorer, marginen M kan sees på som bredden på separasjonen mellom overflatene. Beregning av støttevektoren er et optimaliseringsproblem som kan løses ved hjelp av forskjellige optimaliseringsalgoritmer. Trikset som brukes til å beregne SVM er å bruke forskjellige kjernefunksjoner, som flytter uløselige eller utilstrekkelige problemer til en høyere dimensjon, der det kan løses. I våre eksperimenter trente vi våre SVM-modeller med den sekvensielle minimale optimaliseringsalgoritmen ved hjelp av en lineær kjerne $K(x, y) =< x,y >$ hvor _ = 1.0-12 og toleransen er satt til 0.001, tidligere treningsdata ble normalisert.

For eksperiment 1-funksjoner yter SVM bedre enn C 4,5, presisjonen var 95,8 %. Menneskelige besøkende er fortsatt et problem, selv om SVM har mye høyere frekvens av sanne positive (26,5%). Økt deteksjonsrate for menneskelig besøkende gir en lavere grad av feil deteksjon av roboter (73,5%). F-mål er veldig bra for roboter og mye bedre for menneskelige besøkende (enda bedre enn metode C 4.5) - men fortsatt for lavt til å brukes - (0.419). Med tilleggsfunksjoner Land og ASN (Expertiment 2) oppnådde vi en falsk rate for begge klasser under 5%. Den sanne positive raten var også høy for klasse Human 0,962 og for klasse Robot 0,998. Vi kan konkludere med at med denne delmengden av funksjoner og med regelmessig omskoling for å unngå konseptdrift, er denne modellen mulig for daglig bruk.

Usecase: Skybasert system for hindring av tap av data

Sammenligning av DLP-løsninger tilgjengelig på markedet

Sammenligning av DLP-løsninger tilgjengelig på markedet, basert på Gartner Gartner ® Releases 2022 Market Guide for Data Loss Prevention: Key Takeaways.

Symantec

Symantec er basert i Mountain View i California og har vært på DLP-markedet siden oppkjøpet av Vontu i 2007. Symantec har nylig lansert Symantec Data Loss Prevention 15.0 og har komponentprodukter for DLP Enforce, DLP IT Analytics, skylagring (støtter mer enn 65 skyapplikasjoner), Cloud Prevent for Microsoft Office 365, DLP for endepunkt, DLP for nettverks- og DLP-lagring, samt tredjeparts sikkerhetsteknologi DLP API-støtte, for eksempel henting av innhold, rapportering, og FlexResponse for kryptering av innhold eller DRM-program. Symantec fortsetter å investere i DLP-teknologi og forbedrer forretningsenheten for databeskyttelse. I 2016 kjøpte Symantec Blue Coat, noe som gir selskapet muligheten til å kjøpe Elastica og Perspecsy for Blue Coat, som det er integrering av DLP-policyer for gjennom toveis REST API mellom Elastica og Symantec DLP. Symantec er et praktisk valg for organisasjoner som krever avanserte deteksjonsteknikker og integrering med CASB for en unik databeskyttelsespolicy.

Fordeler

Symantec tilbyr de mest avanserte deteksjonsteknikkene på markedet med avansert funksjonalitet som skjemagjenkjenning, bildeanalyse og håndskriftgjenkjenning som kan dekke et bredt spekter av scenarier for tap av data. Symantec støtter en hybrid distribusjonsmodell for flere av sine DLP-produkter der deteksjonsservere installert på AWS, Azure eller Rackspace kobles til en lokal DLP Enforce-plattform. Symantecs SmartResponse-system tilbyr et bredt spekter av administrativ fleksibilitet basert på innholdshandlinger som samsvarer med DLP-regelen. Dens Vector Machine Learning (VML) DLP gjør det mulig for brukere å lære DLP-systemet ved å gi både positivt og negativt prøveinnhold. Dette kan være nyttig hvis tradisjonelle matchmaking-metoder ikke er tilstrekkelige til å samsvare innholdet riktig.

Svakheter

Symantec-kunder uttrykte frustrasjon når de kjøpte eller oppdaterte Data Insight-plugins for Symantec DLP, som nå eies av Veritas. Sørg for at din Symantec DLP-leverandør også kan selge Veritas Data Insight hvis du er interessert i dette tillegget. Overvåking og oppdagelse av sensitive data i skyprogrammer krever DLP-endepunktsdeteksjon og de nødvendige Symantec CASB-kontaktene for å oppnå full funksjonalitet. Kunder uttrykker bekymring over de totale kostnadene ved å implementere Symantec DLP, sammenlignet med konkurrerende produkter.

Digital verge

Digital Guardian (tidligere Verdasys) ble etablert i 2002 og har hovedkontor i Waltham, Massachusetts. Tilgang til Digital Guardian DLP er hovedsakelig via DLP-endepunktet, med sterke partnerskap for DLP-produktnettverksintegrasjon og DLP-deteksjon innen oktober 2015, da Code Green Networks (CGN) ble kjøpt opp gjennom oppkjøp. Siden den gang har den lansert den som en linje med Digital Guardian Network DLP-produkter. Digital Guardian-endepunktet dekker DLP, avansert trusselbeskyttelse og endepunktsdeteksjon og -respons (EDR) i en enkelt agent installert på stasjonære datamaskiner, bærbare datamaskiner og servere som kjører på Windows, Linux og Mac OS X, samt støtte for VDI-miljøer. Digital Guardian Network DLP og Digital Guardian Discovery-produktet dekker DLP-nettverk, skydatabeskyttelse og dataoppdagelse, og tilbys som maskinvare, programvare og / eller virtuelle apper. I løpet av 2016 jobbet Digital Guardian med å forenkle og integrere administrasjonsfunksjoner mellom sine DLP-endepunkter og eiendeler fra CGN-oppkjøp. Digital Guardian har også et eksisterende partnerskap med Fidelis Cybersecurity Network DLP. Flere Gartner-kunder snakket nylig om dette partnerskapet, og Gartner tror at i tillegg til eksisterende felles kunder, vil partnerskapet fortsette å redusere og til slutt stoppe. Digital Guardian er et passende valg for organisasjoner med sterke bekymringer om lovgivningen, spesielt i helsesektoren og finansielle tjenester, samt organisasjonen med kravene til AD-beskyttelse av immateriell eiendom. Digital Guardian er også et godt valg for organisasjoner som krever ensartethet av DLP-regler for å fungere like bra i alle Windows, Mac OS X og Linux operativsystemer.

Fordeler

Kunder rapporterer raskere implementeringstider og vellykkede prosjekter når de bruker Digital Guardian-produktet i kombinasjon med administrerte digitale vergetjenester. Digital Guardian har integrasjon med bredere sikkerhetsprodukter, inkludert trusseletterretning, nettverkssandkasse, bruker- og enhetsanalyse (UEBA), Cloud Data Protection og Security Event Management (SIEM, inkludert IBM QRadar- og Splunk-applikasjoner). Kunder liker muligheten for modulær lisensiering for DLP-endepunktet, med støtte for Windows, Mac OS X og Linux, og har endepunkter som kan lisensieres i en hvilken som helst kombinasjon av enhetssynlighet og -kontroll, DLP og avansert trusselbeskyttelse. Digital Guardians visjon viser en sterk forståelse av teknologi, sikkerhet, trusler og trender i bransjen som vil forme budene deres.

Svakheter

Digital Guardian har ikke en felles policy for endepunkter og nettverksprodukter. Digital Guardian Agent kan ikke skille mellom personlige og forretningskontoer for Microsoft OneDrive. Det kan imidlertid forhindre bruk av personlige Microsoft OneDrive-applikasjoner. Kunder uttrykte bekymring for hastigheten på integreringen av den oppkjøpte CGN. Indeksering av strukturerte data støttes ikke av Digital Guardian-endepunktagenten, men denne funksjonen er tilgjengelig via CGN-agent.

Kraftpunkt

I 2015 fullførte Raytheon og Vista Equity Partners et joint venture som kombinerer Websense, et porteføljeselskap Vista Equity og Raytheon Cyber Products. I 2016 fikk selskapet to linjer med Intel Security - Stonesoft og Sidewinder fyrverkeri gjennom oppkjøp - og startet det sammenslåtte selskapet som Forcepoint. Raytheon har allerede en kommunal aksje i Forcepoint, og Vista Equity Partners har en minoritetsandel. Forcepoint har hovedkontor i Austin, Texas, og har vært ledende innen DLP-produktmarkedet, tidligere kjent som Raytheon-Websense, i flere år. Forcepoint DLP-produktserien inkluderer Forcepoint DLP Discover, Forcepoint DLP Gateway, Forcepoint Cloud Applications og Forcepoint DLP Endpoint. I løpet av årene med levering av DLP og integrerte DLP-moduler for sine sikre web- og e-postgatewayprodukter, har Forcepoint skapt en enestående DLP-pakke for nettverksdekning, endepunkter og dataoppdagelse (både klient og sky), med spesiell oppmerksomhet på beskyttelse av immateriell eiendom og implementering av samsvarspolicyen med forskriftene. Forcepoint er et egnet valg for organisasjoner med krav til juridisk samsvar og beskyttelse av immaterielle rettigheter, eller organisasjoner som ønsker å implementere virtuelle enheter for hindring av datatap i Azures offentlige skyinfrastruktur.

Fordeler

Forcepoint DLP Endpoint kan automatisk kryptere/dekryptere filer via Microsoft RMS uten å fjerne RMS-beskyttelse basert på ende-til-ende-data, bevegelsesdata og oppdagelsesregler. Forcepoint gir over 350 forhåndsdefinerte regler og innebygd komponent-UEBA for ekstra sikkerhetsanalytiske funksjoner som utfører hendelsesrisikovurdering, identifiserer trusler fra interne brukere, peker ut truede endepunkter og beregner indikatorer for datatyveri for å identifisere de mest sårbare brukerne og aktivitetene. Indeksering av strukturerte data, spesielt dataindekseringsstøtte i Salesforce, nevner klienter som den viktigste differensiatorfaktoren.

Svakheter

Klienter rapporterte problemer med teknisk støtte for indeksering av strukturerte data. Hvis du trenger å indeksere strukturerte data i databasen, må du passe på at du tester dem grundig på aktive data i ditt spesifikke databasemiljø. Raytheons engasjement i forsvarsmarkedet vil bidra til å styrke Forcepoint med ytterligere intelligens og produkter. Det er imidlertid ingen suksess for sikkerhetsleverandører eid av forsvarsstrukturer som har lyktes i kommersielle markeder. Forcepoints relevans i noen geografiske områder kan være problematisk på grunn av Raytheons sterke amerikanske lojalitet. Noen Gartner-kunder har notert seg denne klagen og ser om dette forårsaker bekymringen din i organisasjonen din.

Intel Security (i dag: McAfee)

I løpet av de siste årene har Intel endret sin investering i og fra ulike produktlinjer flere ganger, og har ikke tilstrekkelig vurdert disse endringene i og utenfor selskapet. Dette har forårsaket utmattelse av ansatte i alarmerende hastigheter, hvorav mange har blitt lansert av nye sikkerhetsselskaper eller er ansatt av konkurrerende sikkerhetsleverandører. Historisk sett har det i mange av Intels sikkerhetsprodukter vært en kronisk mangel på investeringer.

Intels sikkerhetstilnærming var å integrere anskaffelser med McAfees policystyringssystem ePolicy Orchestrator (McAfee ePO), varslingsovervåking og koble sikkerhetshendelser mellom DLP-hendelsesslutter, nettverksoverføringer og begrensede data om lagringsdata i organisasjonen. DLP 10.0-utgivelsen har ført til ytterligere forbedringer av DLP, og oppdateringer av DLP-nettprodukter i 2016 fremhevet McAfees fornyede fokus på databeskyttelse. Intel Security er et godt valg for organisasjoner som har betydelige ressurser investert i McAfee ePO og ønsker en unik leverandør som kan tilby DLP, enhetskontroll og kryptering.

Fordeler

DLP-integrering i McAfee Web Gateway-proxy støtter dekryptering og rekryptering av trafikk på nettstedet, inkludert e-posttjenesteleverandører og skylagringsprodukter. Fangstdatabasen kan indeksere og lagre alle synlige nettverks- og endepunktkomponenter. Klienter rapporterte dette nyttig for å teste nye regler, rettsmedisinsk analyse av hendelser som skjedde før politikkutforming og etterforskning etter hendelsen. Den støtter også e-discovery og eldre oppbevaring, samt integrering direkte med programvaren Guidance Software og AccessData. McAfee DLP inkluderer det grunnleggende nivået av dataklassifisering på DLP 10-endepunktet for Windows og Mac OS X, og kan fortsatt integreres godt med Titus og Bold James for ulike dataklassifiseringsalternativer. DLP-endepunktregler er klar over steder og kan ha forskjellige svar og innholdsløsninger når de er tilkoblet når de er frakoblet. Federation of Security Innovations (SIA) er fortsatt robust og er en god måte for Intel Security-kunder å maksimere sine DLP-investeringer på grunn av bevist og testet integrasjon av dataproduktklassifiseringer, DRIF- og UEBA-leverandører.

Svakheter

McAfee DLP støtter opprinnelig API-integrasjon med Cloud Data Box, men støtte for andre skyprogrammer og skylagringsstøtte mangler. Intel Security har gjort noen forbedringer av DLP Agent 10 på Mac OS X, men mangler fortsatt støtte for e-post, Internett og nettsky. Linux støttes ikke. Kunder rapporterer at konfigurasjonen av DLP-regler kan være kompleks og ufordelaktig sammenlignet med andre DLP-produkter. Den fremtidige suksessen til Intel Security i DLP-markedet vil avhenge av deres ytelse mens de opptrer som et selskap, og om fokuset kan være på datasikkerhetsoppgaver over en lengre periode.

Usecase: Dynamisk web hosting

Inspirert av: https://www.linkedin.com/pulse/host-dynamic-website-aws-sara-mostafa/

Hvordan distribuere et dynamisk nettsted med AWS ved å laste opp innholdet på nettstedet ditt i S3-beholder, opprett en EC2-instans for å være vert for webapp på den, som i dette scenariet fungerer EC2 som en offentlig server, alle mennesker fra hele verden kan besøke denne serveren.

Amazon S3 (Simple Storage Service) er en tjeneste som tilbys av AWS for objektlagring via et webtjenestegrensesnitt. Den kan brukes til å lagre eller hente hvilken som helst mengde data som dokumenter, bilder, videoer osv. S3 beholder er en ressurs i Amazon S3. Det er en beholder der filer og mapper kan lastes opp.

Amazon EC2 (Elastic Compute Cloud) er en tjeneste som tilbys av AWS. Det regnes som en virtuell server.

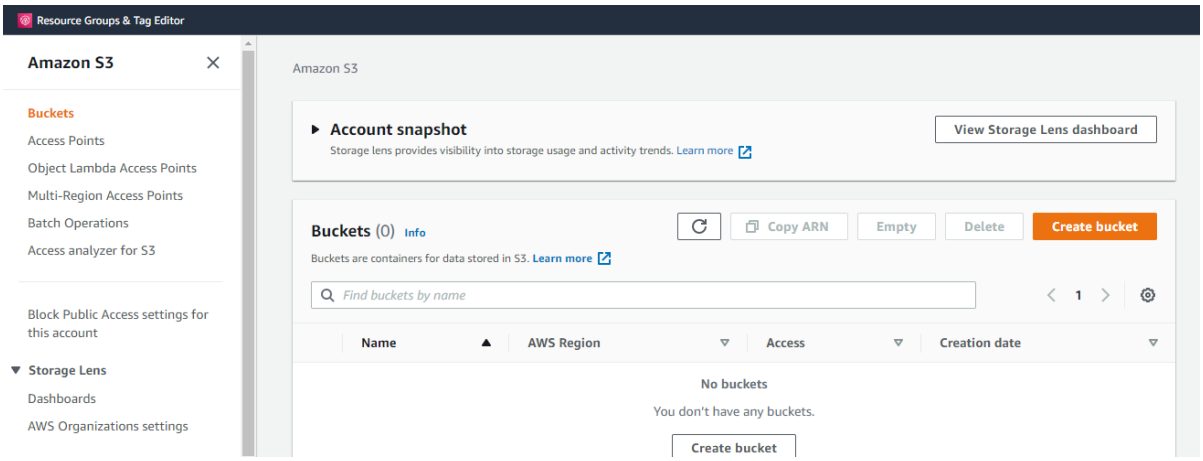
IAM (Identity and Access Management) Rolle brukes til å gi tillatelse til service for å gjøre noe på en annen tjeneste.

LAMP-webserver kan brukes til å være vert for et statisk nettsted eller distribuere et dynamisk PHP-program som leser og skriver informasjon til en database.

Trinn

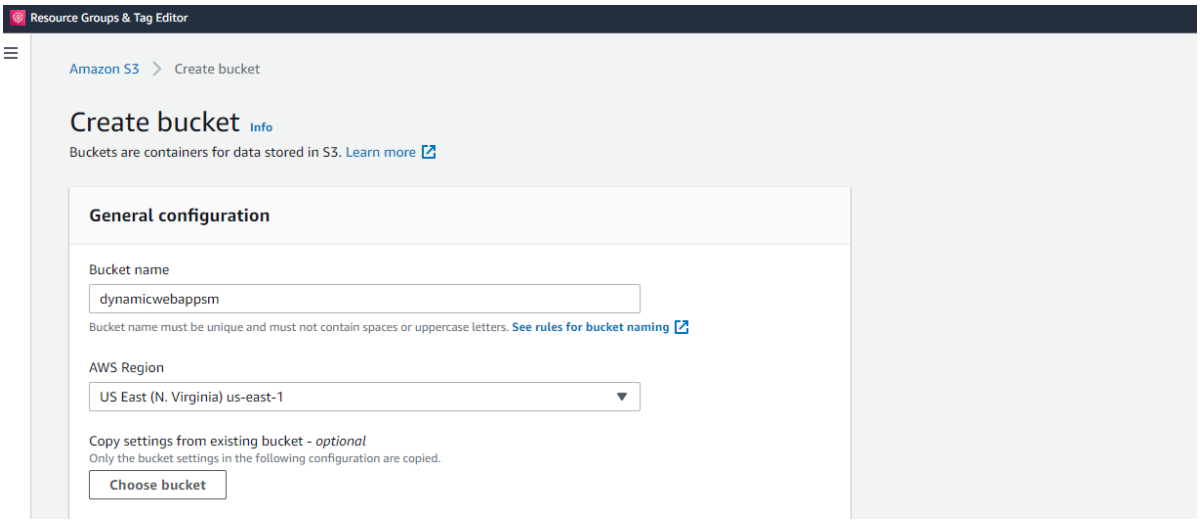
Trinn 1: Opprett S3-beholder

Du må opprette en S3-beholder for å sette nettstedets filer og mapper. For å gjøre dette, logg inn på AWS-administrasjonskonsollen og klikk på Tjenester øverst i navigasjonsfeltet. Fra rullegardinmenyen Tjenester velger du S3 fra delen Lagring. Dette skal vise S3-dashbordet.



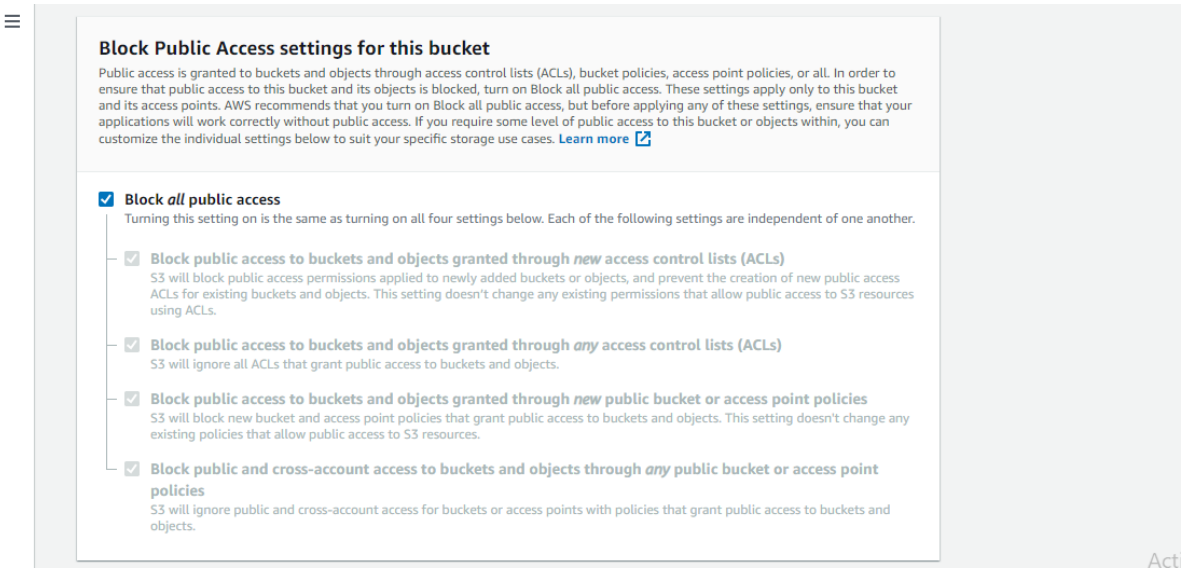
Figur 0.16. Opprette en S3-beholder - første trinn

Fra S3-dashbordet klikker du på Opprett beholder. Gi bøtta et unikt navn, navnet du velger må være globalt unikt. Velg deretter din foretrukne AWS-region fra rullegardinmenyen.



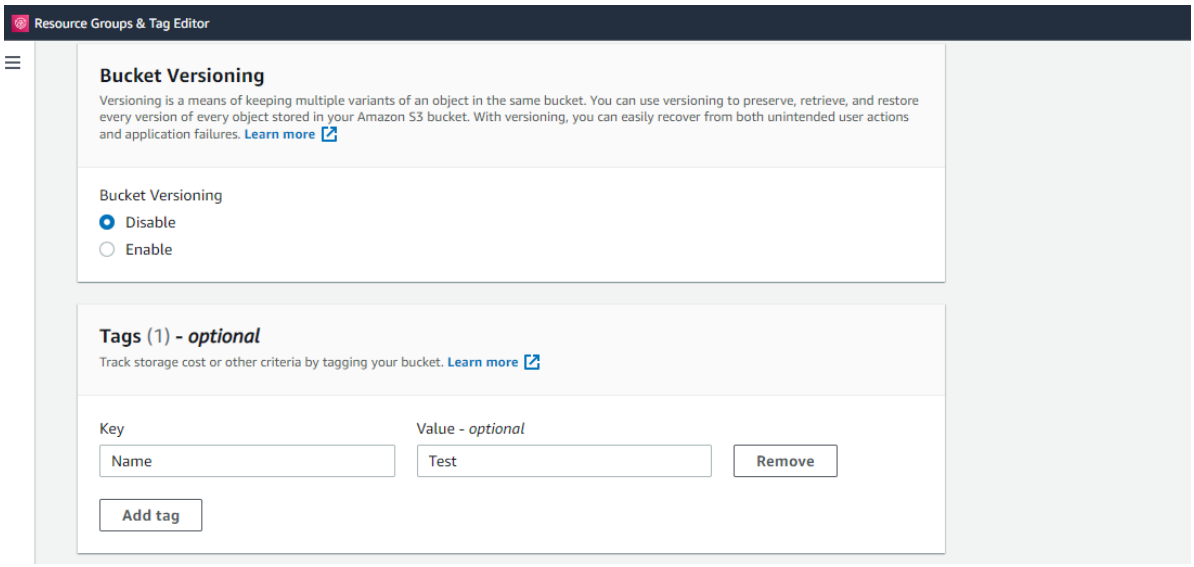
Figur 0.17. Opprette en S3-beholder - andre trinn

Under Blokker innstillinger for offentlig tilgang for denne samlingsdelen merker du av for Blokker all offentlig tilgang. Dette gjøres for å gjøre bøtta ikke tilgjengelig for publikum.



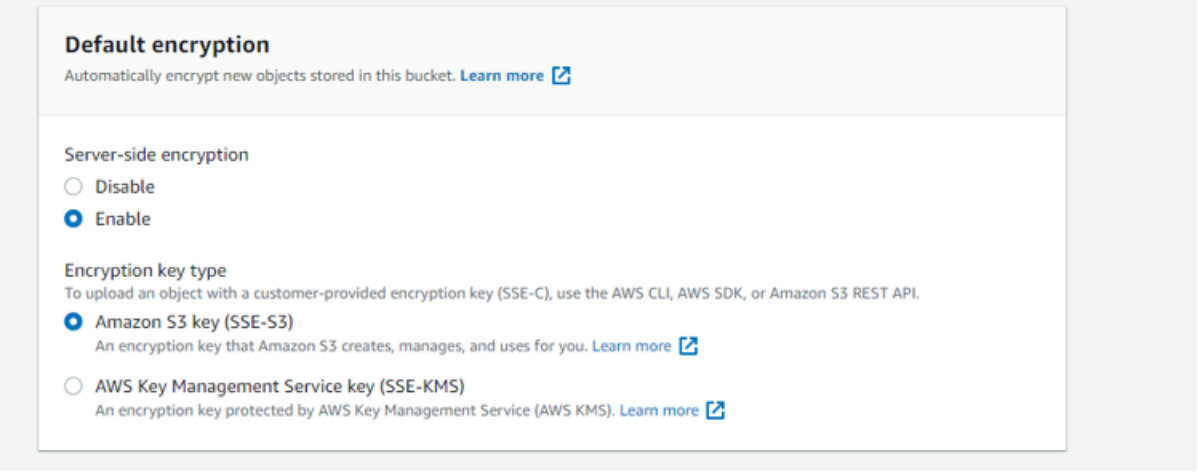
Figur 0.18. Opprette en S3-beholder - tredje trinn

Klikk på Deaktiver for beholder versjonering. Du kan også legge til tagg i samlingen for enkel identifisering.



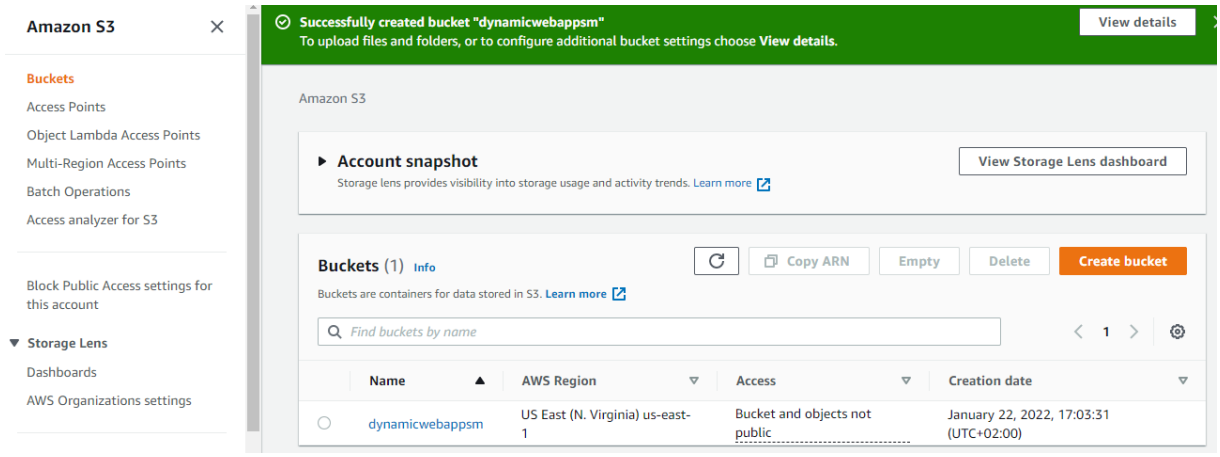
Figur 0.19. Opprette en S3-beholder – fjerde trinn

Under Standard kryptering klikker du på Aktiver for kryptering på serversiden. Sjekk deretter Amazon S3-nøkkel (SSE-S3).



Figur 0.20. Opprette en S3 beholder - femte trinn

Klikk deretter på Opprett beholder.

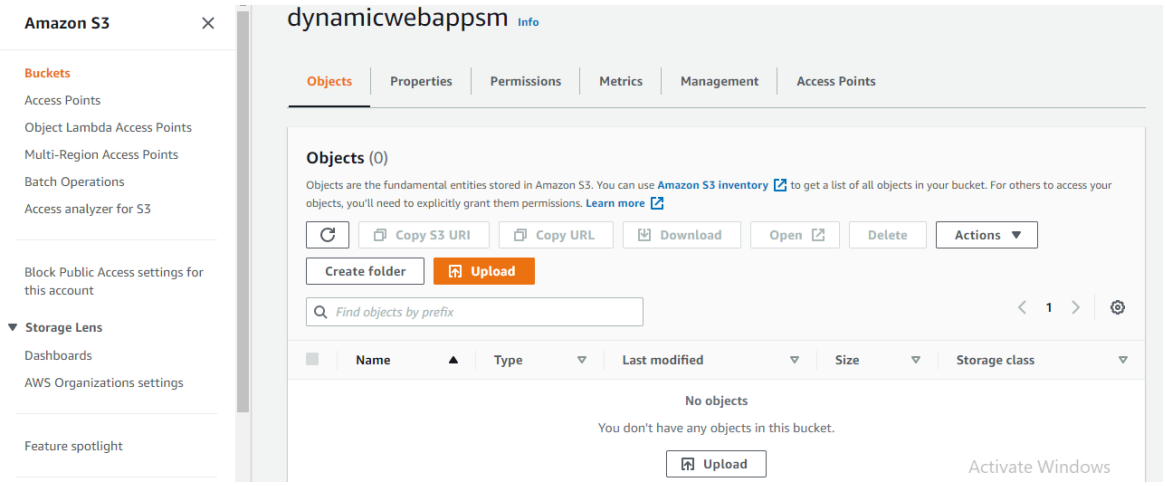


Figur 0.21. Opprette en S3-beholder - sjette trinn

Trinn 2: Last opp webfiler til S3 beholder

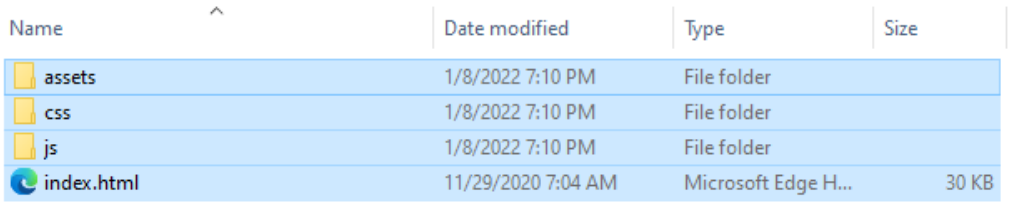
Etter at du har opprettet bøtta, må du laste opp nettstedets filer og mapper til den.

Fra S3-dashbordet klikker du på navnet på bøtta du nettopp opprettet. På objektfanen kan du se at bøtta for øyeblikket er tom, klikk på Last opp-knappen.

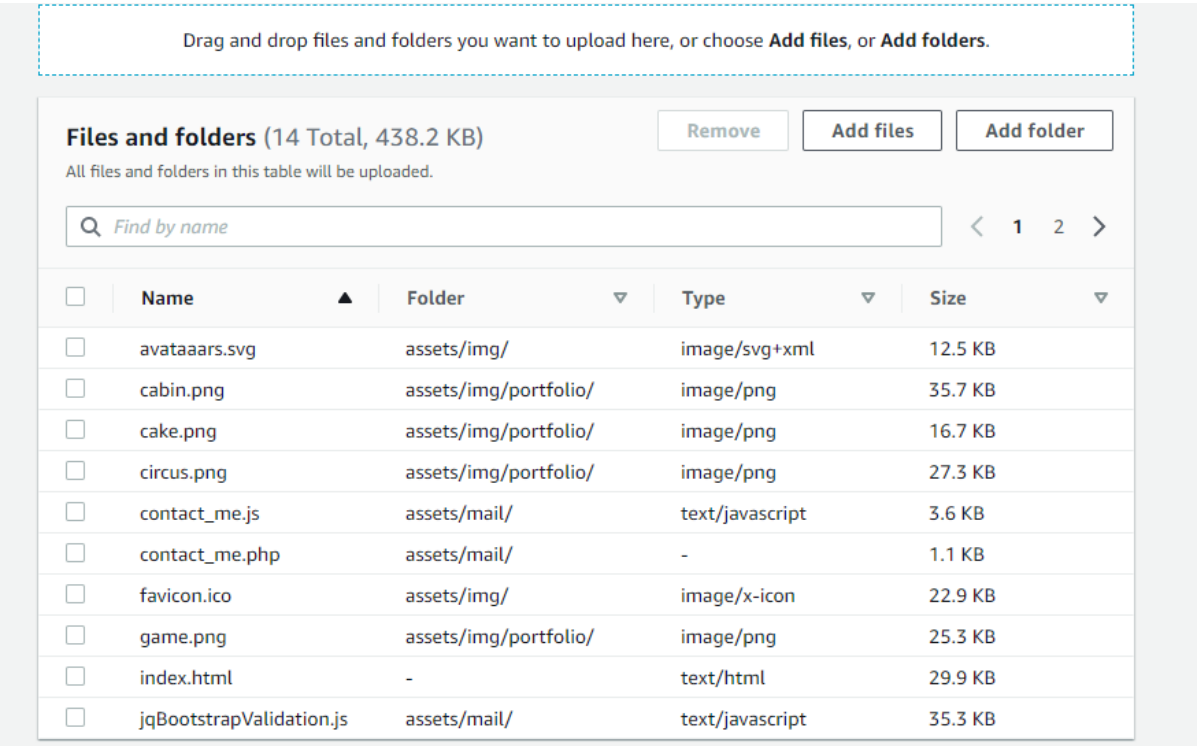


Figur 0.22. Last opp webfiler til S3 beholder - første trinn

Dette bør ta deg til Last opp-siden.



Figur 0.23. Last opp webfiler til S3 beholder - andre trinn

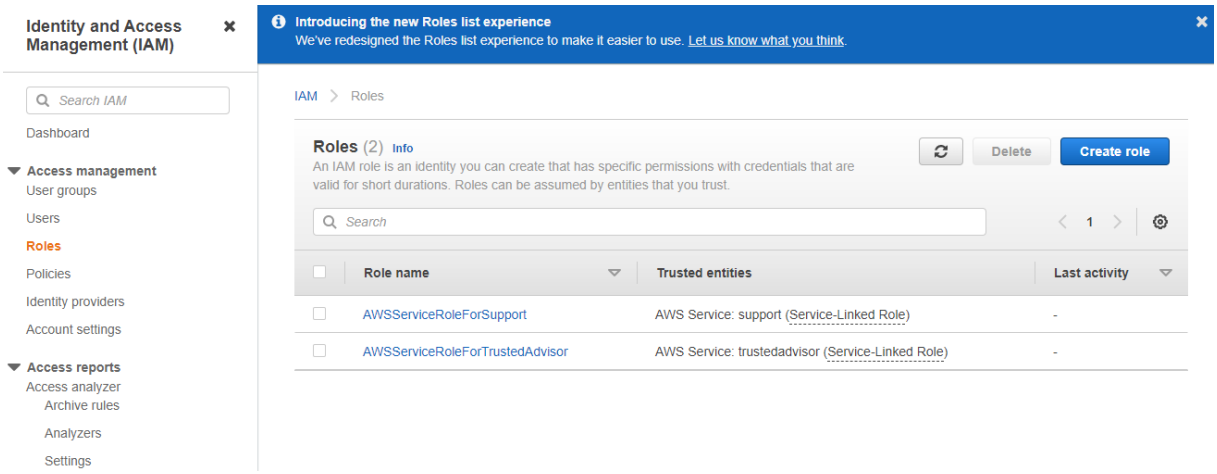


Figur 0.24. Last opp webfiler til S3 beholder - tredje trinn

Etter at de nødvendige filene og mappene er lagt til, blar du ned og klikker på Last opp. Opplastingen bør gjøres om noen få minutter, avhengig av nettverket og innholdsstørrelsen. Ikke lukk fanen mens opplastingsprosessen pågår.

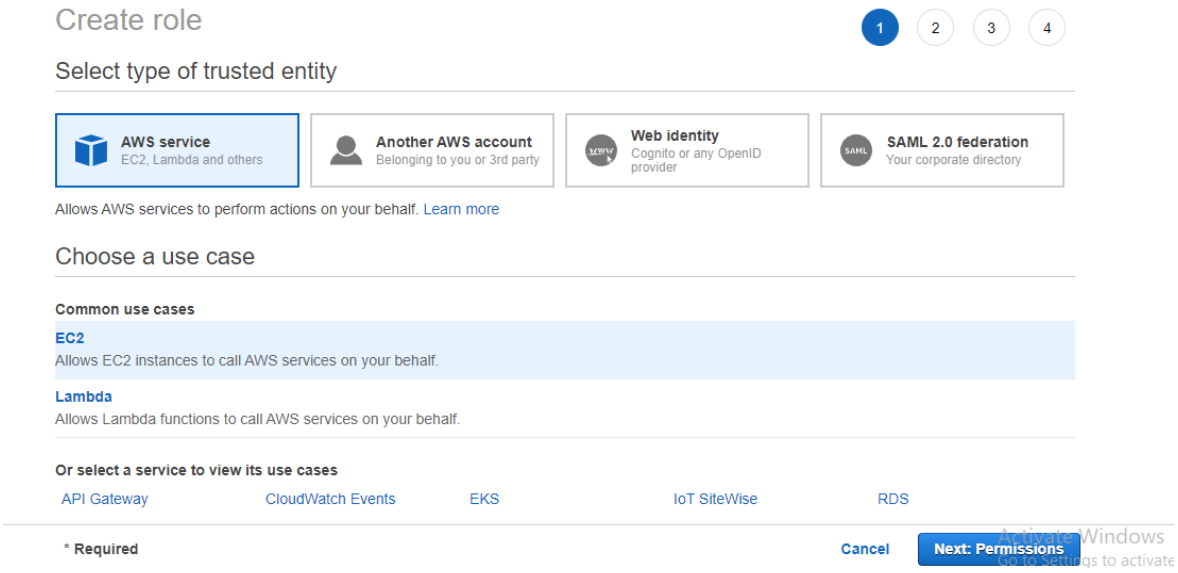
Trinn 3: Opprett IAM-rolle

Nå vil EC2 hente kode fra S3. Så du vil opprette IAM-rolle for å gi EC2 tilgang til S3. Hvis du vil gjøre dette, velger du IAM fra rullegardinmenyen Tjenester, fra delen Sikkerhet, identitet og samsvar. Fra IAM-dashbordet klikker du på Roller. Klikk deretter på Opprett rolle.



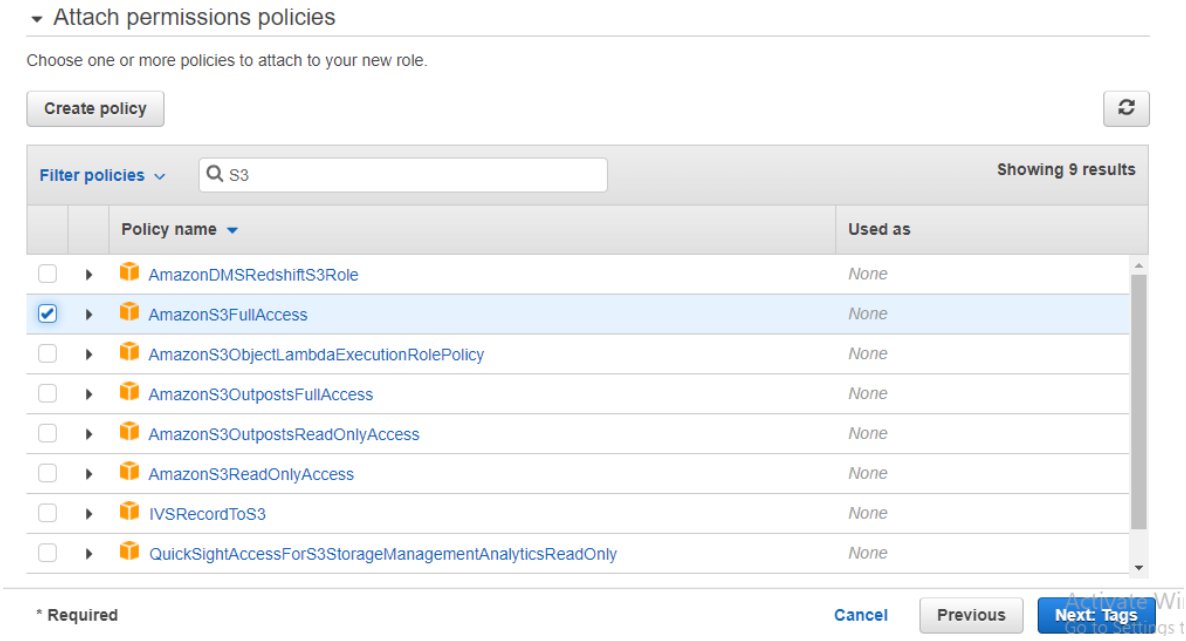
Figur 0.25. Opprett IAM-rolle – første trinn

Velg EC2 og klikk på Neste: Tillatelser.



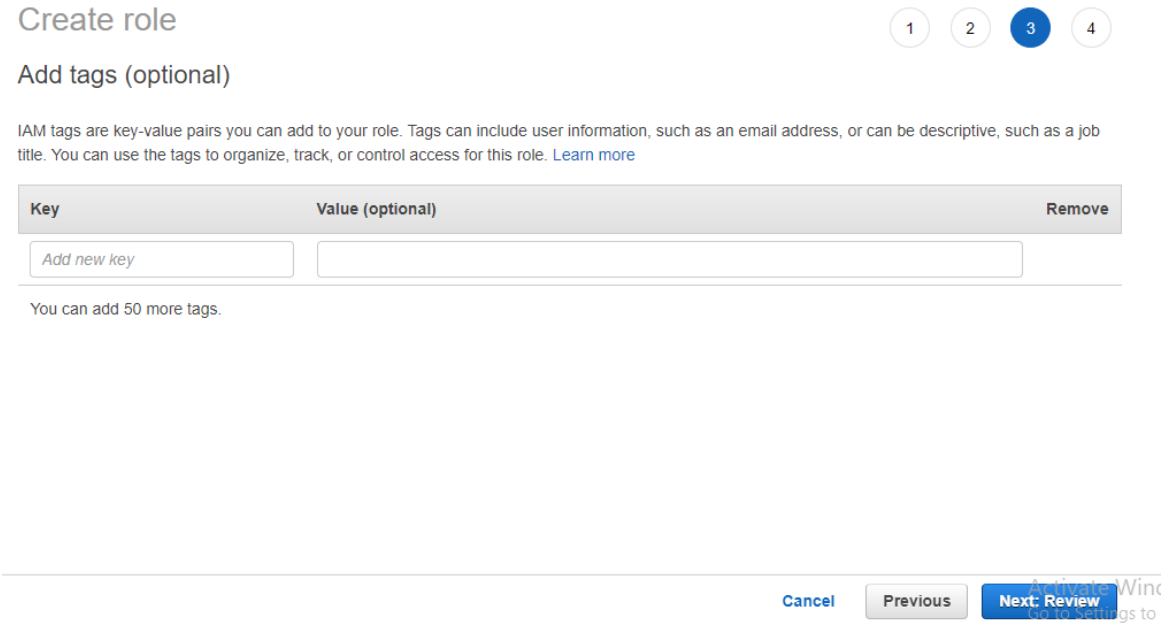
Figur 0.26. Opprett IAM-rolle – andre trinn

Søk etter S3 og sjekk AmazonS3FullAccess. Klikk deretter på Neste: Tagger.



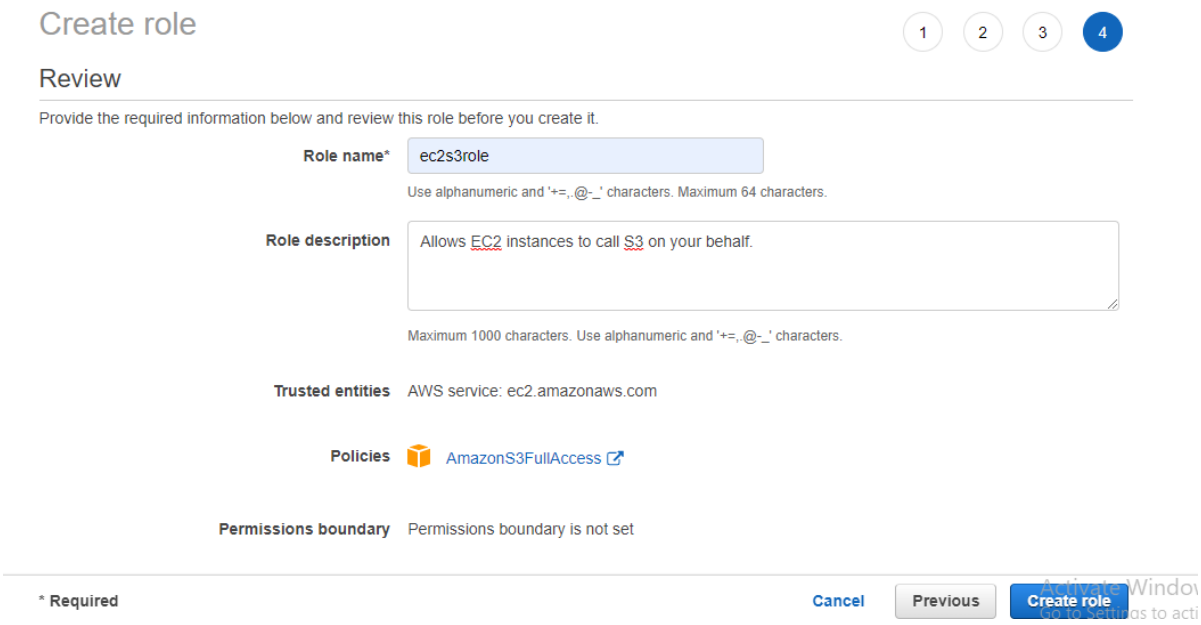
Figur 0.27. Opprett IAM-rolle – tredje trinn

Klikk på Neste: Review.



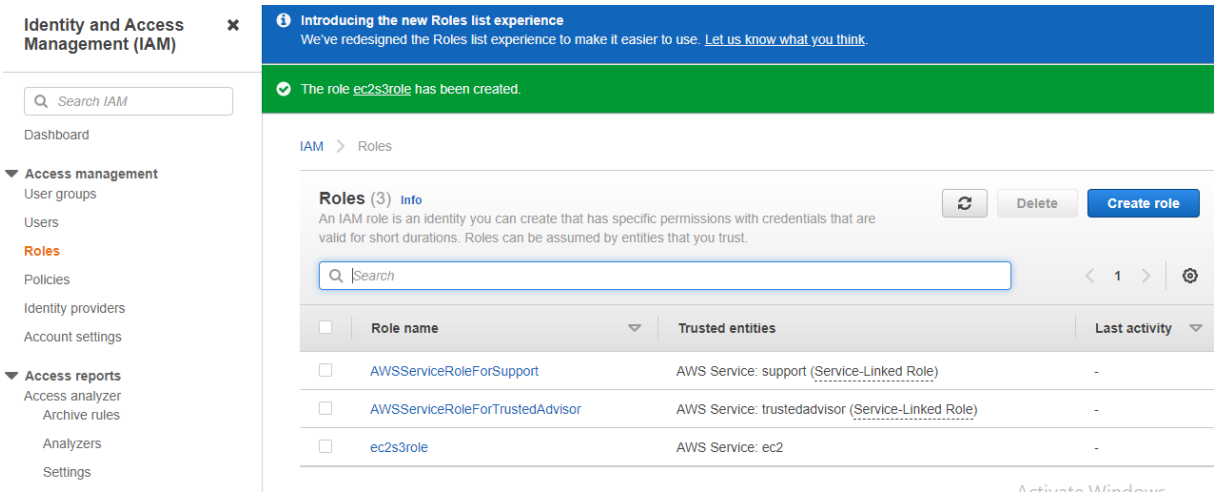
Figur 0.28. Opprett IAM-rolle – fjerde trinn

Gi rollenavnet og beskrivelsen. Klikk deretter på Opprett rolle.



Figur 0.29. Opprett IAM-rolle – femte trinn

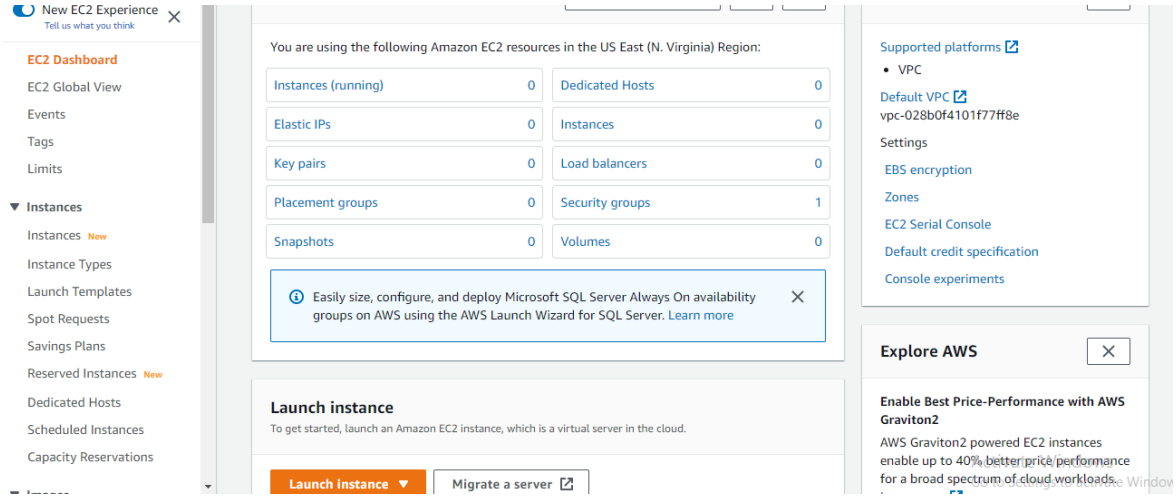
Nå er rollen opprettet vellykket.



Figur 0.30. Opprett IAM-rolle – sjette trinn

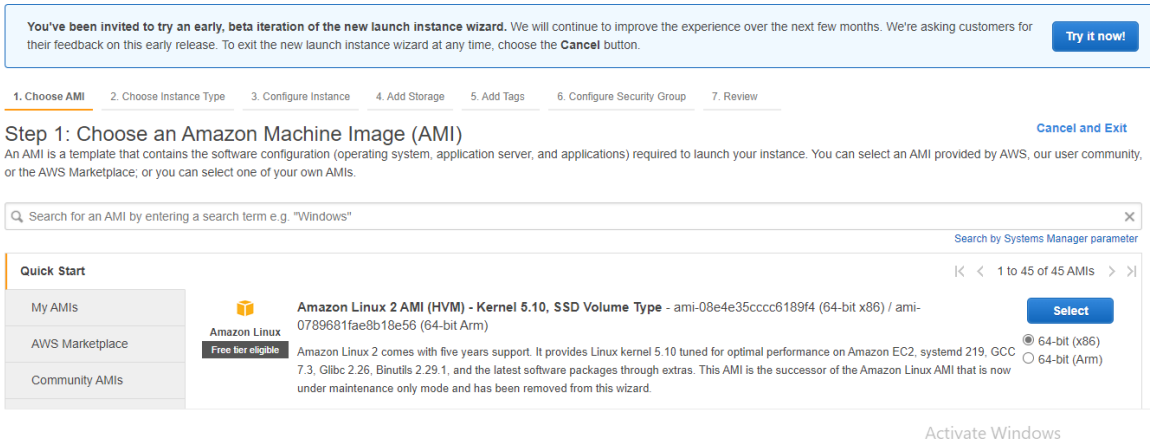
Trinn 4: Opprett en EC2-instans

Du må opprette en EC2-instans for å installere apache (/var/www/html) og kopiere innholdet i S3 til html-katalogen. Dette gjør du ved å velge EC2 fra rullegardinmenyen Tjenester fra delen Beregning. Dette skal vise EC2-dashbordet. Fra EC2-dashbordet klikker du på Start instans.



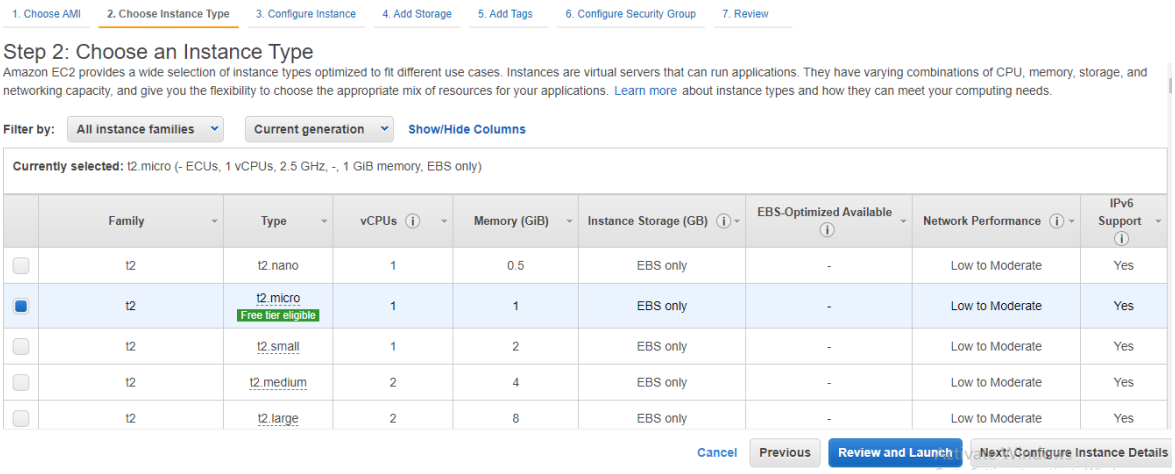
Figur 0.31. Opprett en EC2-instans – første trinn

For AMI, velg Hurtigstart og klikk på Velg for Amazon Linux (Gratis nivå kvalifisert).



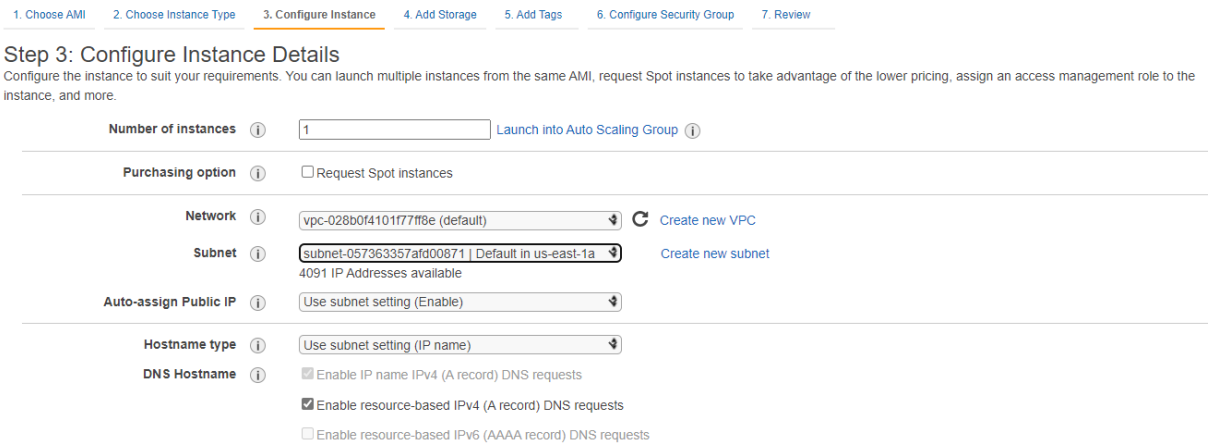
Figur 0.32. Opprett en EC2-instans – andre trinn

For en eksempeltype velger du t2.micro (Free-nivå kvalifisert). Og klikk på Neste: Konfigurer instansdetaljer.



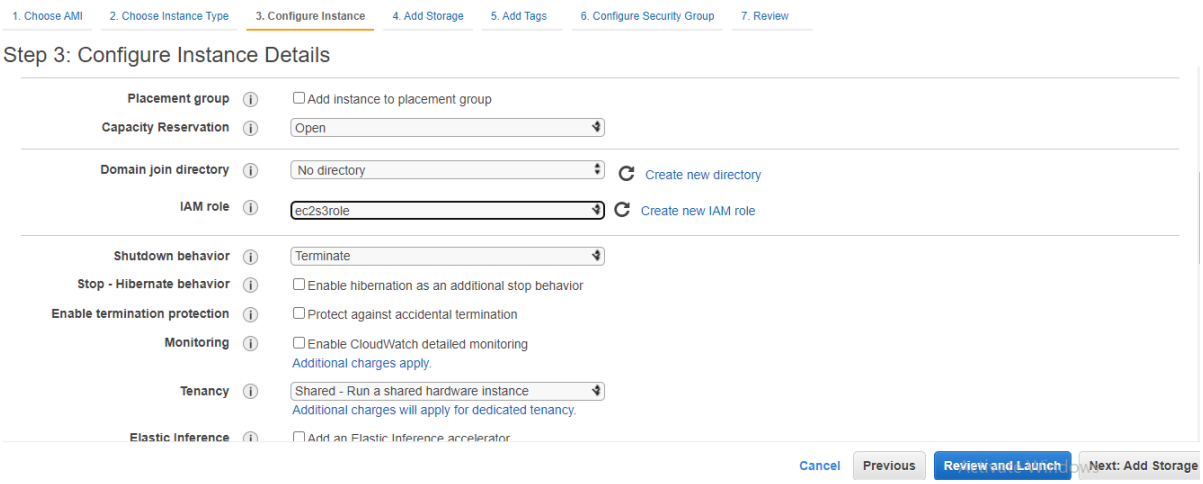
Figur 0.33. Opprett en EC2-instans – tredje trinn

Bestem 1 for Antall instanser, Standard VPC for Nettverk og Standard i US-AST-1a for Delnett.



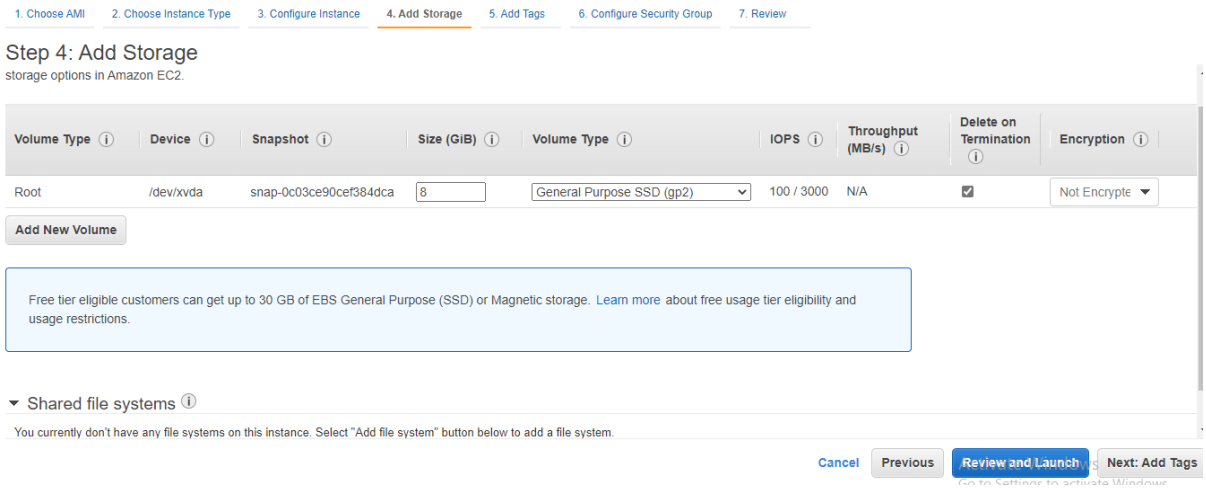
Figur 0.34. Opprett en EC2-instans – fjerde trinn

Velg ec2s3role eller hva du navnga for IAM-rollen. og avslutte for nedleggelsesadferd. Klikk deretter på Neste: Legg til lagring.



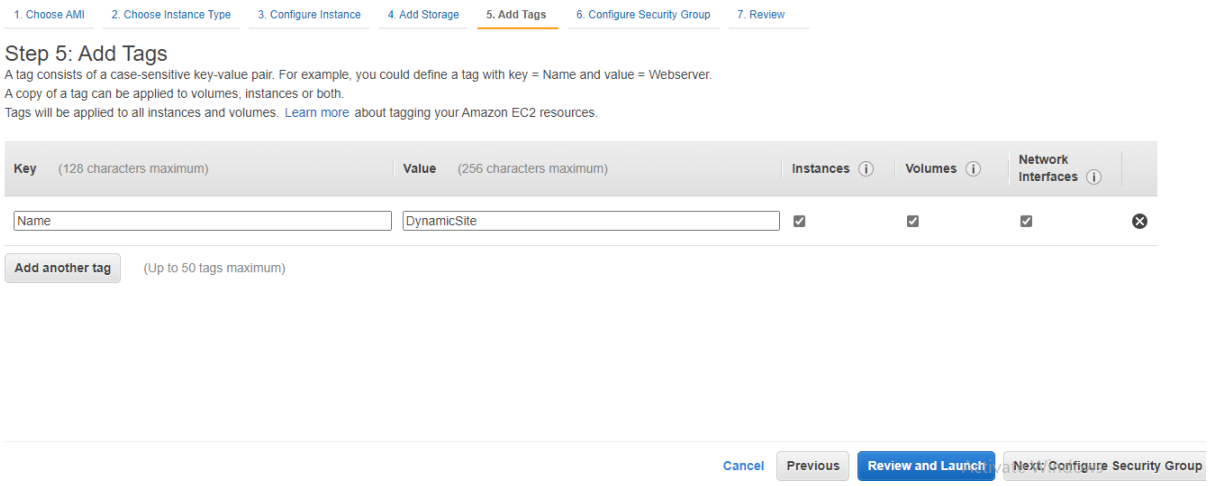
Figur 0.35. Opprett en EC2-instans – femte trinn

Klikk på Neste: Legg til tagger.



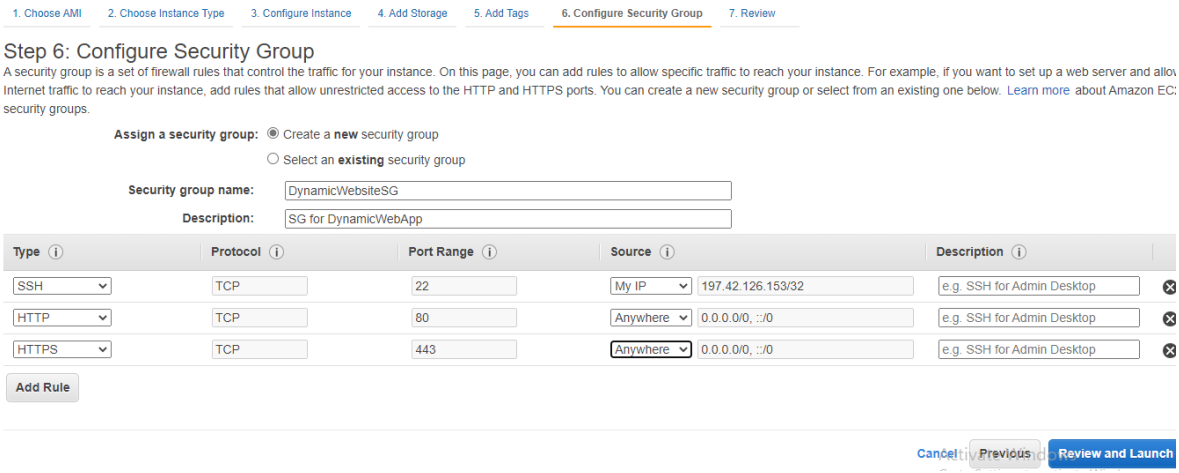
Figur 0.36. Opprett en EC2-instans – sjette trinn

Du kan legge til tag Name: DynamicSite. Klikk deretter på Neste: Konfigurer sikkerhetsgruppe.



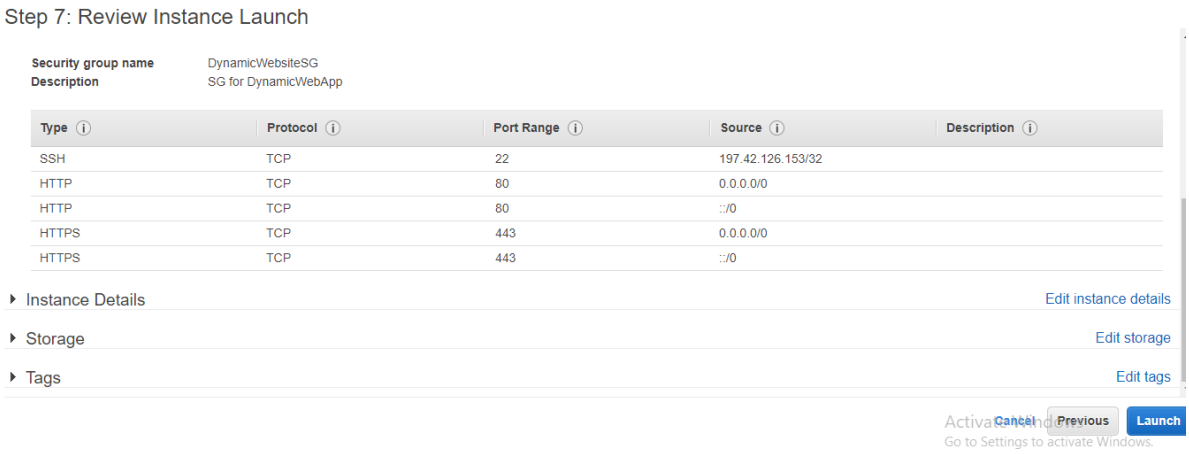
Figur 0.37. Opprett en EC2-instans – syvende trinn

Velg Opprett en ny sikkerhetsgruppe. Gi det navn: DynamicWebsiteSG og beskrivelse: SG for DynamicWebApp. For SSH-regel velger du Min IP for kilde. Klikk på Legg til regel og velg HTTP for Type og hvor som helst for kilde. Siste regel: velg HTTPS for Type og Anywhere for Source. Klikk på Review og Launch.



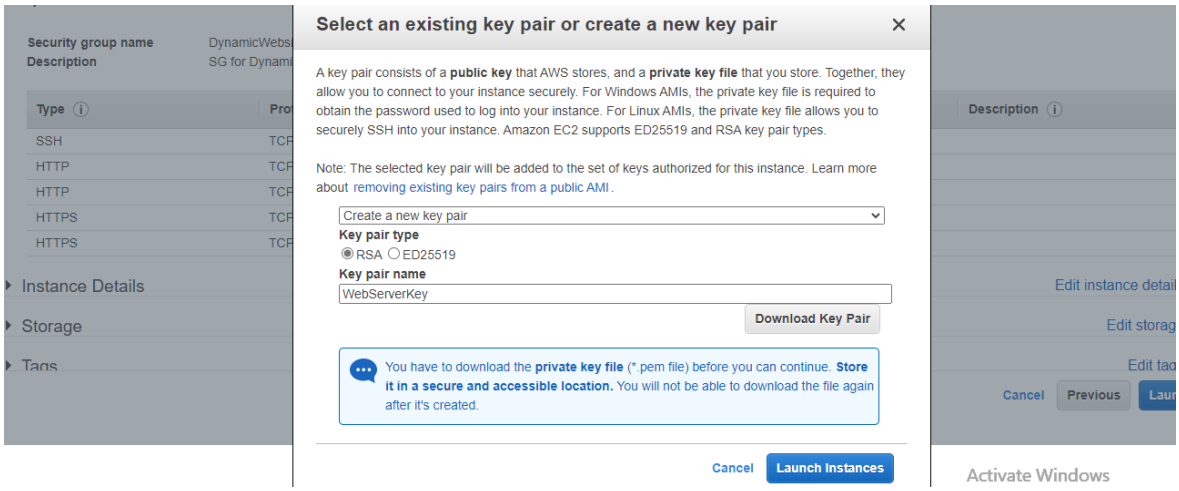
Figur 0.38. Opprett en EC2-instans – åtte trinn

Klikk på Start.



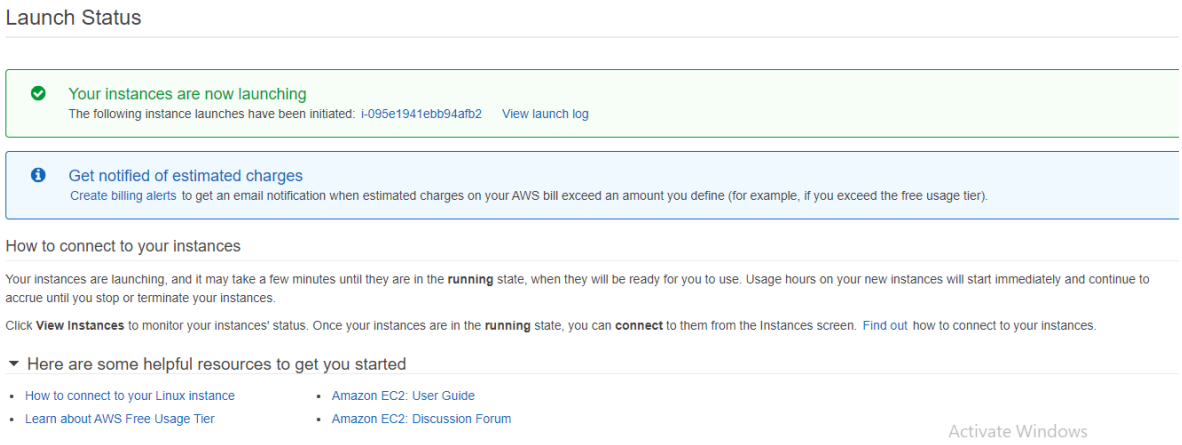
Figur 0.39. Opprett en EC2-instans – niende trinn

Velg Opprett et nytt nøkkelpar og RSA for type. Gi den navnet WebServerKey og klikk på Download Key Pair. Merk: Du bør laste ned nøkkelen til SSH på EC2. Klikk på Start instanser.



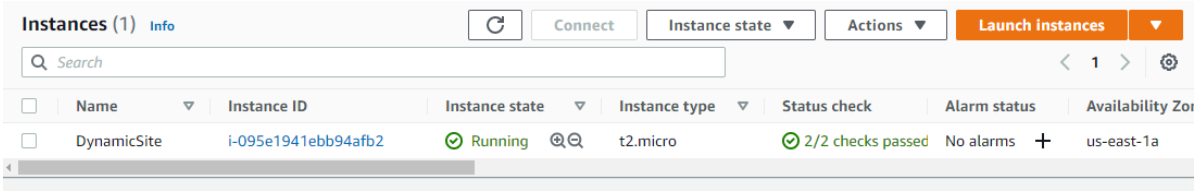
Figur 0.40. Opprett en EC2-instans – tiende trinn

Nå lanseres instansen.



Figur 0.41. Opprett en EC2-instans – ellevte trinn

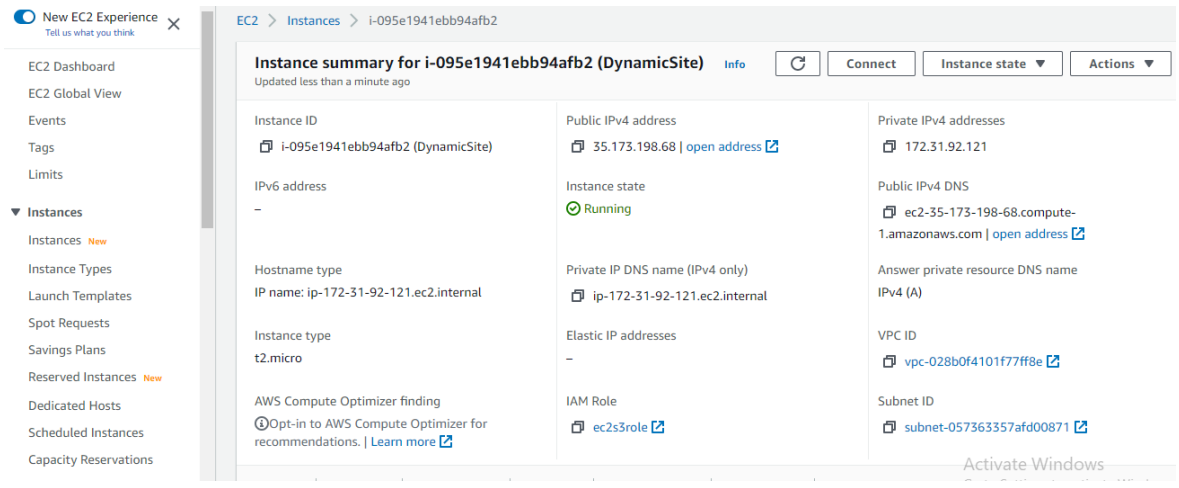
Klikk på Review Instance og vent Statussjekk vil være 2/2 sjekker bestått.



Figur 0.42. Opprett en EC2-instans – siste trinn

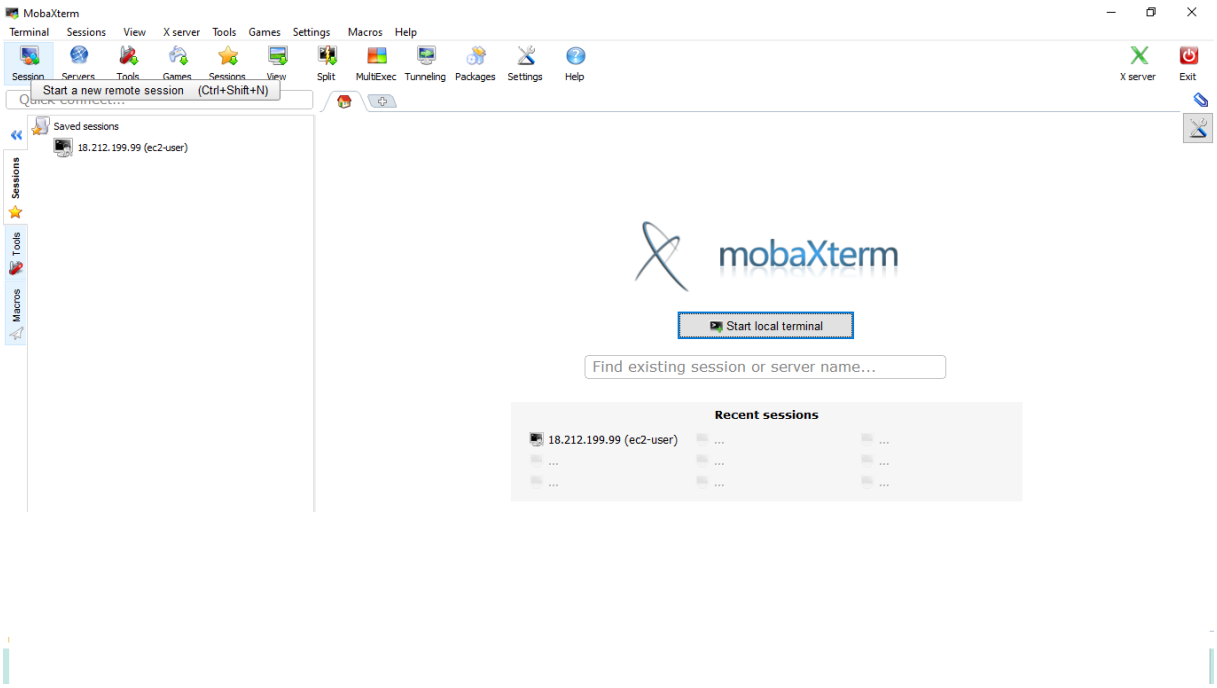
Trinn 5: SSH med MobaXterm

Nå vil du koble til EC2 ved hjelp av MobaXterm. Først bør du kopiere den offentlige IPv4-adressen til EC2-instansen.



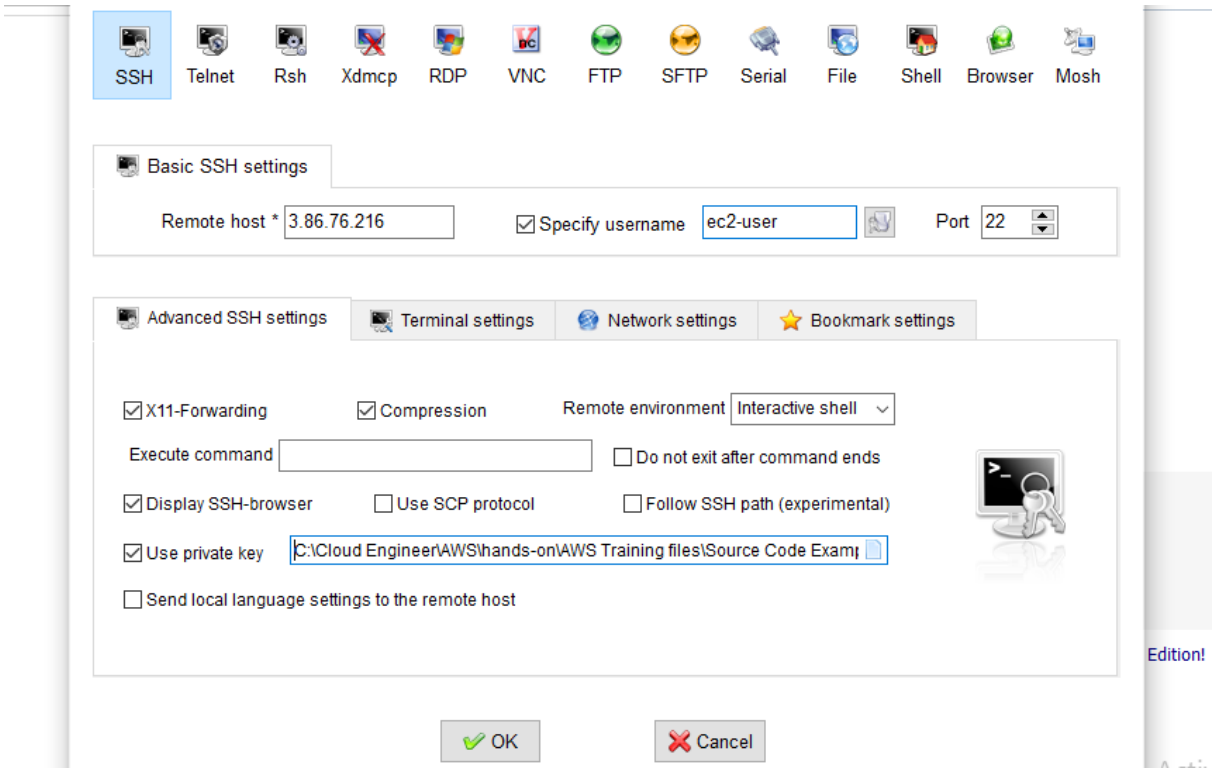
Figur 0.43. Koble til EC2 ved hjelp av MobaXterm – første trinn

Åpne MobaXterm og start en ny ekstern økt ved å klikke på Økt.



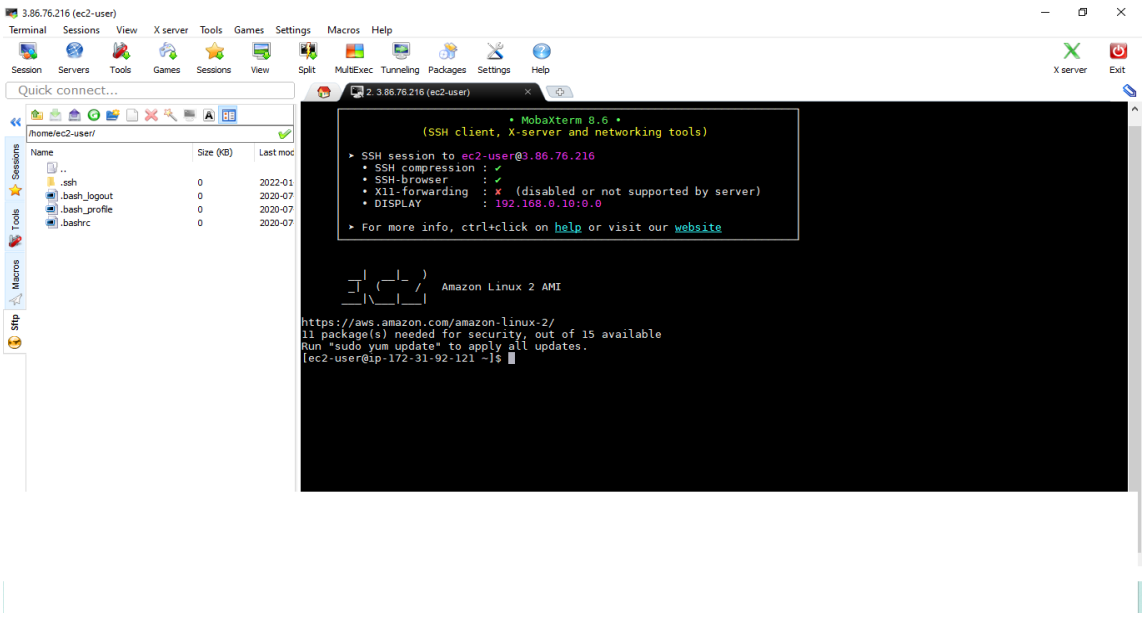
Figur 0.44. Koble til EC2 ved hjelp av MobaXterm - andre trinn

Klikk på SSH. Lim inn IP av EC2 For eksempel: (3.86.76.216). Og ec2-bruker for Angi brukernavn. Klikk på Avanserte SSH-innstillinger, sjekk Bruk privat nøkkel og bla gjennom plasseringen av nøkkelen. Klikk OK.



Figur 0.45. Koble til EC2 ved hjelp av MobaXterm – tredje trinn

Nå har du koblet til EC2.



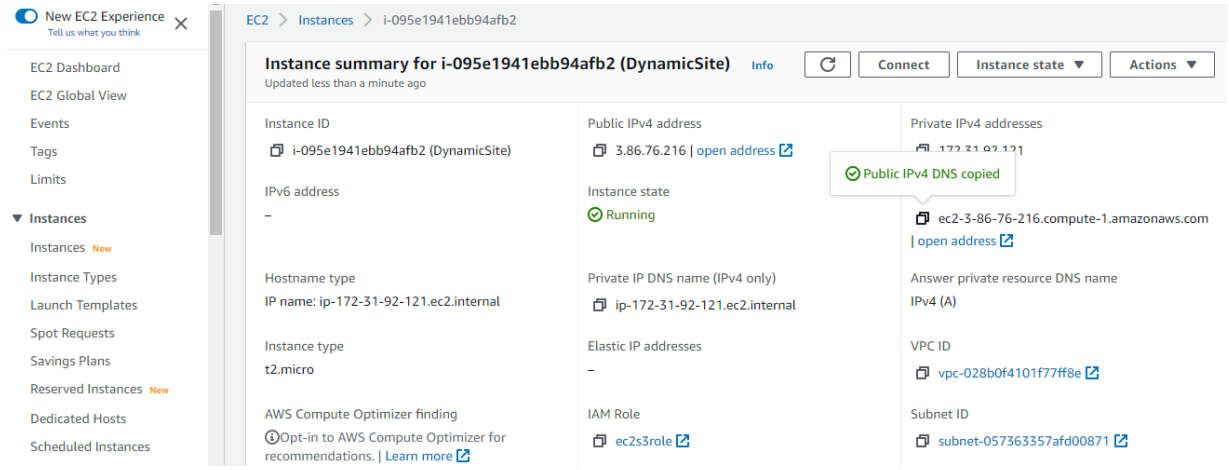
Figur 0.46. Koble til EC2 ved hjelp av MobaXterm – fjerde trinn

Trinn 6: Installer en LAMP-webserver på Amazon Linux 2

Følgende prosedyrer hjelper deg med å installere en Apache-webserver med PHP og MariaDB.

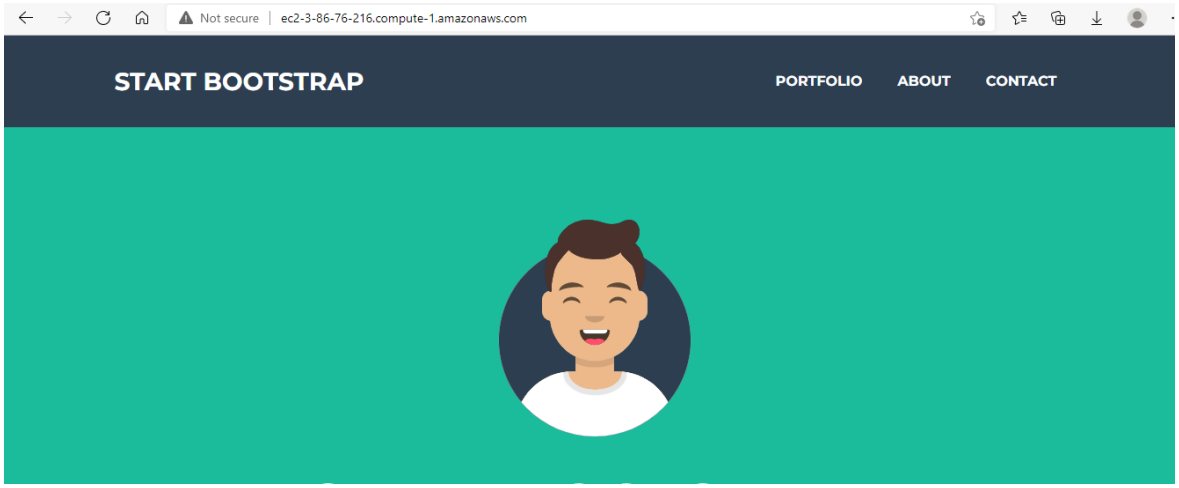
```
#update the instance
sudo yum update -y
#Install the lamp-mariadb10.2-php7.2 and php7.2 Amazon Linux Extras repositories to
#get the latest versions of the LAMP MariaDB and PHP packages for Amazon Linux 2.
sudo amazon-linux-extras install -y lamp-mariadb10.2-php7.2 php7.2
#Now you can install the Apache web server, MariaDB and PHP software packages.
sudo yum install -y httpd mariadb-server
#Start the Apache web server.
sudo systemctl start httpd
#Use the systemctl command to configure the Apache web server to
#start at each system boot.
sudo systemctl enable httpd
#You can verify that htppd is on by running the following command.
sudo systemctl is-enabled httpd
#Now, you want to copy the content of the website from the S3 bucket
#to the directory /var/www/html in EC2.
#Make sure you copy your S3 bucket name.
sudo aws s3 cp s3://YOUR_BUCKET_NAME/ /var/www/html/ --recursive
#To verify that the content is copied to the directory, run the following command.
cd /var/www/html
ls
```

Kopier offentlig IPv4 DNS og lim den inn i en ny fane.



Figur 0.47. Installere en LAMP-webserver på Amazon Linux 2

Gratulerer, du har distribuert et dynamisk nettsted på EC2 vellykket.



Figur 0.48. Vellykket distribusjon av et dynamisk nettsted på EC2

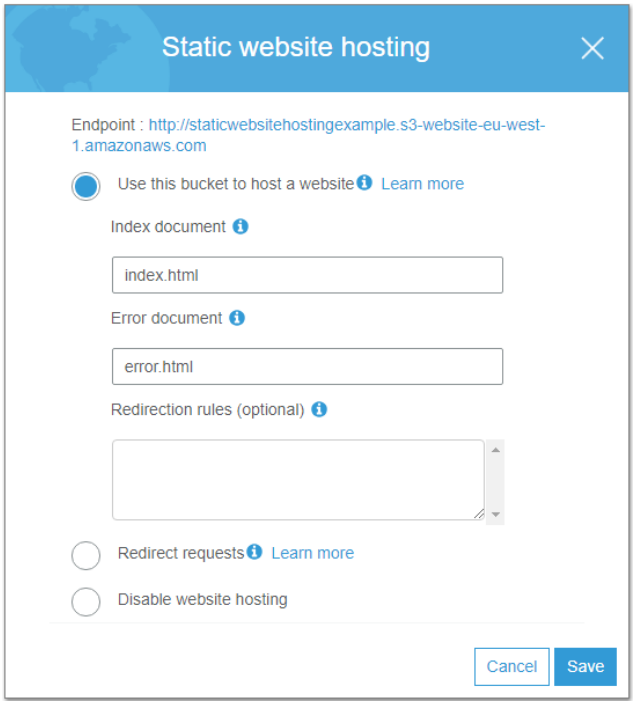
Usecase: Host et statisk nettsted ved hjelp av AWS (eller andre sky-leverandører)

Trinn-for-trinn-guide

Grunnleggende konfigurasjoner

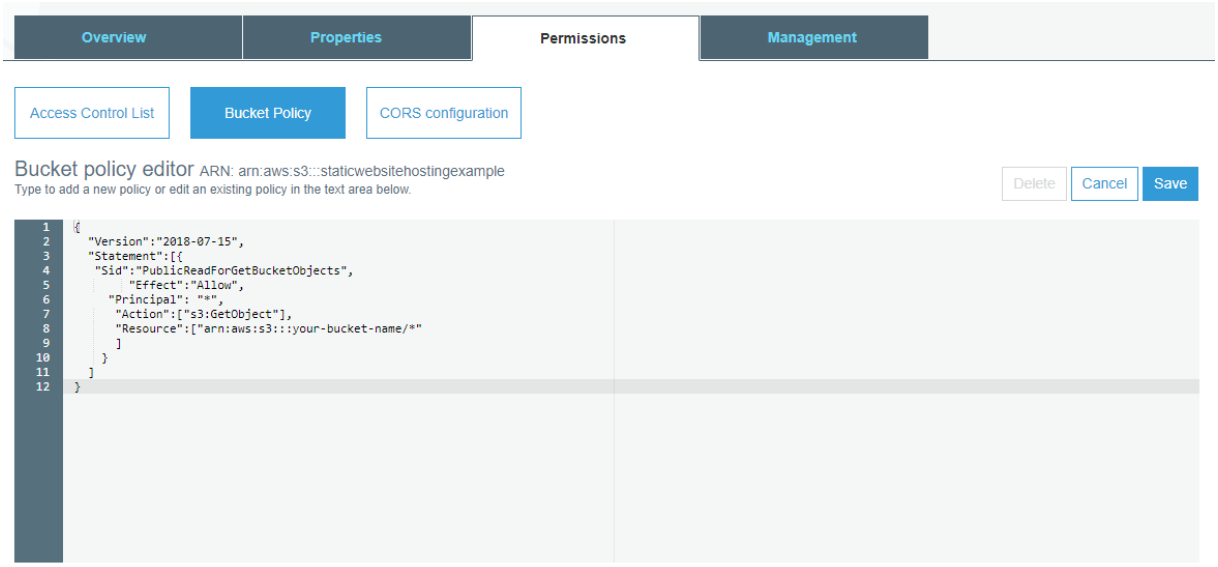
1. Gå til S3-konsollen og opprett en ny beholder med standardinnstillinger.
2. Gå egenskapene til bøtta og velg alternativet "Statisk webhotell."
3. Aktiver alternativet "Bruk denne beholdern til å være vert for et nettsted."
4. Angi navnene på HTML-koden som skal vises som hjemmeside, og HTML-filen som skal vises i tilfelle det oppstår en feil på området.

Du kan eventuelt angi omadresseringsregler hvis du vil rute forespørsler betinget i henhold til bestemte objektnøkkelnavn, prefikser i forespørselen eller svarkoder til et annet objekt i samme verdiområde eller ekstern URL.



Figur 0.49. Host et statisk nettsted ved hjelp av AWS - første trinn

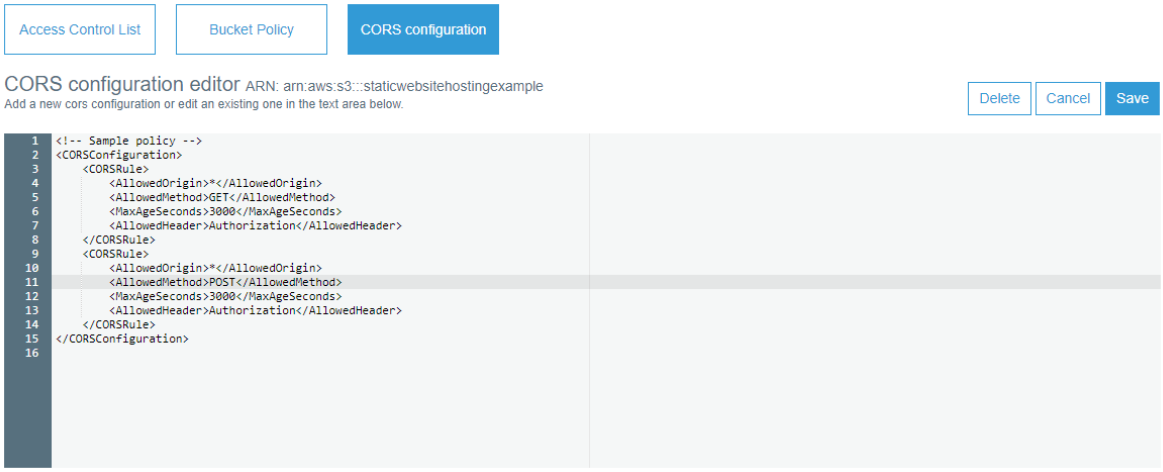
Gå nå til Tillatelser-delen av beholder og legg til følgende i Bucket Policy-delen:



Figur 0.50. Host et statisk nettsted ved hjelp av AWS - andre trinn

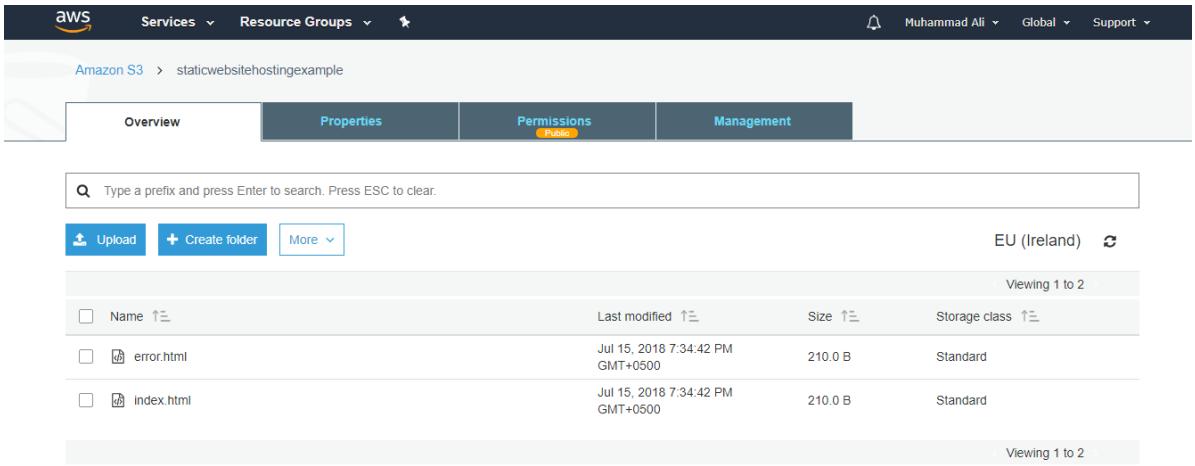
Bytt *ut beholdernavnet ditt* med navnet på bøtta di.

For å aktivere ditt S3 statiske nettsted for å svare på forespørsler som GET og POST som kommer fra et eksternt program som er vert på et bestemt domene, må du konfigurere CORS i beholderinnstillingene. Hvis du vil gjøre dette, legger du til følgende i CORS-konfigurasjonsdelen av Tillatelser:



Figur 0.51. Host et statisk nettsted ved hjelp av AWS - tredje trinn

Last opp koden din. For denne opplæringen, lage to enkle HTML-filer ved navn indeks.html og feil.html og laste dem opp til beholder.



Figur 0.52. Host et statisk nettsted ved hjelp av AWS - fjerde trinn

For å starte og teste nettstedet kan endepunktet hentes fra Properties > Static website hosting.

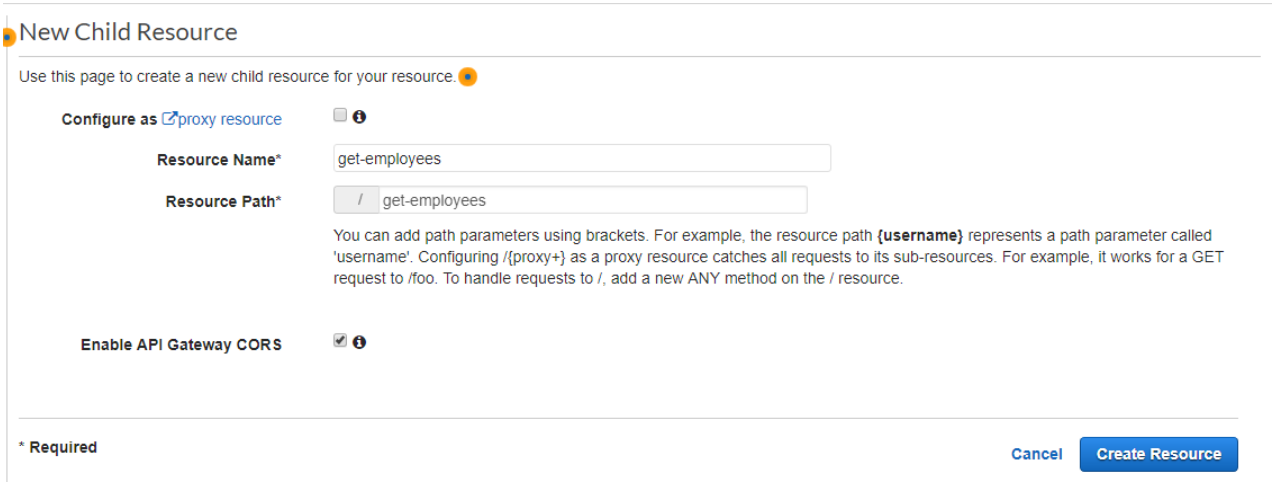
Berik nettstedet ditt ved å legge til dynamisk atferd

Du kan bruke en kombinasjon av HTML5 og CSS3 for å berike nettstedet ditt grafisk. Du kan også bruke jQuery Ajax til å spørre en API (mikrotjeneste) for å dynamisk hente data fra en datakilde og vise den på nettstedet ditt. På samme måte, ved å aktivere API-endepunkter ved hjelp av Ajax, kan du lagre alle typer brukerdata tilbake til datakilden, som alle andre webprogrammer. Hvis kravet ditt er å bruke AWS bare for alle utviklingsbehovene dine, kan du bruke en kombinasjon av API Gateway og Lambda til å bygge API-er, en veiledning som du finner her.

CORS-innstillinger i API-gatewayendepunkter

Det er viktig å merke seg at når du utvikler APIer (mikrotjenester) ved hjelp av en API Gateway og Lambda, må du sørge for å gjøre følgende:

Aktiver CORS i API-gatewayen når du oppretter en ny ressurs.



Figur 0.53. Host et statisk nettsted ved hjelp av AWS - femte trinn

Når du skriver lambda-funksjonen (som du vil integrere med API Gateway-endepunktet for å gi funksjonalitet til mikrotjenesten), må du sørge for å legge til en ekstra parameter i svarhodet med navnet Access-Control-Allow-Origin med verdien **"*"**