CADRU EDUCAȚIONAL PRIVIND CLOUD COMPUTING

Prima parte

A-CCT

Cofinanțat de Uniunea Europeană

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

CADRU EDUCAȚIONAL PRIVIND CLOUD COMPUTING

Prima parte

Novo mesto, 2023

Cofinanțat de Uniunea Europeană

DOI: 10.37886/a-cct-ro

CADRU EDUCAŢIONAL PRIVIND CLOUD COMPUTING – PRIMA PARTE

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

Sprijinul Comisiei Europene pentru producerea acestei publicații nu constituie o aprobare a conținutului, care reflectă doar opiniile autorilor, iar Comisia nu poate fi făcută responsabilă pentru nici o utilizare a informațiilor conținute în aceasta publicatie care ar putea fi făcută.

Publicat de: Faculty of Organization Studies in Novo Mesto

Accesibil la: https://www.fos-unm.si/si/dejavnosti/zaloznistvo/

Kataložni zapis o publikaciji (CIP) pripravili v Narodni in univerzitetni knjižnici v Ljubljani
COBISS.SI-ID 178828035
ISBN 978-961-6974-89-9 (PDF)

Cofinanțat de Uniunea Europeană

2021-1-SI01-KA220-VET-000034641

Conținut

CONȚINUTUL FIGURILOR

Cofinanțat de Uniunea Europeană

2021-1-SI01-KA220-VET-000034641

Cofinanțat de Uniunea Europeană

2021-1-SI01-KA220-VET-000034641

DICȚIONAR

Expresie	Expresie englezesc	Sens
Agilitate	*Agility*	Agilitatea în contextul cloud computing se referă la adaptarea rapidă și eficientă a resurselor și serviciilor cloud la cerințele de afaceri și tehnologice în evoluție.
Hinterlandul/Backend	*Backend*	Componentele serverului unei aplicații cloud. Acesta acoperă multe funcționalități, cum ar fi gestionarea datelor, implementarea logicii de afaceri, găzduirea aplicațiilor și procesarea datelor. Aceste componente back-end funcționează împreună cu front-end-ul orientat către utilizator pentru a facilita funcționarea și funcționalitatea acestuia.
Rețea de interconectare /Backhaul	*Backhaul*	Columna vertebrală a rețelei servește drept canal pentru transmiterea datelor către nucleul central al rețelei.
Date de rezervă	*Back-up data*	Dublarea datelor este procesul de creare a unei copii suplimentare a datelor care este deja stocată într-o altă locație pentru a reduce riscul de pierdere a datelor.
Blockchain	*Blockchain*	Un registru distribuit care înregistrează toate tranzacțiile care au loc în rețea.
Blowfish	*Blowfish*	Pentru a asigura transferul securizat al datelor, se folosește un cifru bloc cu o cheie simetrică.
Găleată	*Bucket*	O entitate logică pentru stocarea datelor în sistemele de stocare a obiectelor, cum ar fi AWS S3.
Cloud computing	*Cloud computing*	Exploatarea resurselor de calcul precum servere, stocare și baze de date printr-o infrastructură de internet denumită în mod obișnuit „clorul”.
Tehnologii de cloud computing	*Cloud computing technologies*	Tehnologii care facilitează utilizarea serviciilor informatice prin Internet.
Cluster	*Cluster*	O rețea de computere interconectate care lucrează strâns împreună pentru a efectua activități.
Durabilitate	*Durability*	Durabilitatea datelor se referă la capacitatea sistemului de a preveni pierderea datelor într-un interval de timp specificat.

Elasticitate	*Elasticity*	Abilitatea de a aloca dinamic resurse de calcul pe baza volumului de lucru predominant.
Firewall	*Firewall*	Un dispozitiv de securitate a rețelei care îndeplinește funcțiile de monitorizare și filtrare atât a traficului de rețea de intrare, cât și de ieșire.
Flexibilitate	*Flexibility*	Abilitatea de a se adapta eficient și flexibil la schimbările și fluctuațiile volumului de muncă.
În față	*Frontend*	Componente care se referă la interfața cu utilizatorul și experiența utilizatorului într-un sistem dat.
Flux	*Flux*	Flux este o nouă generație de infrastructură cloud descentralizată scalabilă.
Anteturi	*Headers*	Un preambul, folosit de obicei pentru a include informații de rutare, este un set suplimentar de date situat la începutul unui pachet de date.
Controale de sănătate	*Health checks*	Starea curentă sau starea funcțională a unui sistem sau proces.
Sondă de sănătate	*Health probe*	Implementarea sistemelor de control este esențială pentru a asigura că Serviciile funcționează la cel mai înalt nivel de eficiență.
Hub	*Hub*	O interfață utilizată pe scară largă pentru stabilirea conectivității între dispozitivele dintr-o rețea.
Revolutia industriala	*Industrial revolution*	Timpul menționat marchează o fază importantă a dezvoltării industriale, posibil sugerând conceptul de Industrie 4.0 în cadrul tehnologiei informaționale moderne. Această paradigmă cuprinde integrarea IoT și cloud computing.
Tehnologia IT	*IT technology*	Utilizarea sistemelor informatice și a tehnologiilor de telecomunicații pentru stocarea, preluarea, transmiterea și manipularea datelor.
Latența	*Latency*	Întârzierea de timp care apare în sistem.
Ascultător	*Listener*	Un sistem sau un protocol de monitorizare a rețelei care detectează în mod activ și răspunde la conexiunile și solicitările de rețea.
Rețea locală de calculatoare	*Local computer network*	O rețea locală (LAN) se referă la o rețea care acoperă o zonă geografică limitată, cum ar fi o casă, un loc de muncă sau o instituție de învățământ.
Computer cu cadru principal	*Main frame computer*	Un sistem de calcul de înaltă performanță utilizat pentru a efectua sarcini de calcul intensive la scară largă.

Cartografiere	*Mapping*	Procesul de stabilire a unei relații între elementele aparținând unei mulțimi și elementele aparținând altei mulțimi.
Plasture	*Patch*	O actualizare de software menită să-și corecteze sau să-și îmbunătățească funcționalitatea.
Proxy	*Proxy*	Un server intermediar care acționează ca intermediar între clienții utilizatorilor finali și destinațiile pe care le accesează în scopuri de navigare.
Apăsați codul	*Push code*	Acțiunea de a transfera cod într-un depozit sau într-un mediu cu scopul de a face modificări.
Dirijare	*Routing*	Procesul de determinare a căii pentru transmiterea pachetelor de date în cadrul unei rețele.
Scalabilitate	*Scalability*	Capacitatea sistemului de a se extinde și de a gestiona în mod adecvat nivelurile crescute de cerere.
Seturi de scară de mașini virtuale	*Virtual machine scale sets*	Resursa de calcul Azure menționată mai sus este o platformă care permite utilizatorilor să implementeze și să controleze o colecție de mașini virtuale (VM-uri) care nu se pot distinge.
Mașini virtuale	*Virtual machines*	O simulare de sistem computerizat este o reprezentare software care imită capacitățile unui computer fizic.

1 INTRODUCERE

În anul 2021, partenerii de proiect din Slovenia, Regatul Țărilor de Jos, Norvegia, România, Croaţia și Turcia au primit cu success aprobarea pentru proiectul european Erasmus+ intitulat: „Digital content development for integration of cloud technologies in formal and distance vocational education" (Dezvoltare de materiale digitale pentru integrarea tehnologiilor de cloud computing în învăţământul formal şi la distanţă). Unul dintre rezultatele proiectului este și conținutul materialelor didactice ale cursurilor despre tehnologiile cloud, susținute de aplicații eșantion, pregătite ca ghid pentru profesorii din învățământul profesional formal și la distanță. Mai jos, profesorii pot găsi o primă parte a ghidurilor menționate.

În acest document, profesorii vor găsi o serie de propuneri de valoare pe care partenerii de proiect le-au identificat ca fiind cele mai potrivite pentru a începe să predea studenților despre serviciile cloud. Accentul s-a pus pe convergența industriilor astăzi, astfel încât profesorii vor găsi o combinație de bune practici din diferite industrii pentru a oferi studenților soluții personalizate cu eficiență maximă pentru studenții lor. Subiectele conținutului materialului didactic în cloud sunt următoarele: 1. Introducere în cloud computing și tipuri de cloud computing, 2. Preț vs comparație de piață între AWS, Azure și GCP, 3. Implementarea serverelor și a Load Balancers (echilibratorilor de încărcare) pe toate platformele de calcul, 4 .Servicii de stocare pe AWS, Azure și GCP, 5.Servicii de securitate - Gestionarea identității și accesului, 6.Tipuri de servicii de rețea și setarea acestora, 7.Servicii de bază de date pe AWS, Azure și GCP, 8.Configurare domeniu și 9.Monitorizare și Serviciul de notificare.

De asemenea, profesorul poate găsi mai jos 61 de exemple practice de aplicații, potrivite pentru predarea tehnologiilor cluod către studenții din învăţământul profesional. În anexa 1, profesorul poate găsi un exemplu mai detaliat de aplicații, iar în anexa 2, poate găsi fragmente de cod pentru unele dintre aplicațiile de mai jos, pe care profesorii le pot folosi ca modele care le uşurează explicaţiile pentru studenții din învăţământul tehnic profesional (VET) şi pot aplica modelele prin utilizarea codurilor.

2 MATERIALE DE PREGĂTIRE PENTRU CLOUD COMPUTING

2.1 Introducere în tehnologiile cloud computing şi tipurile de cloud computing

Nivel de dificultate: uşor
Durata de studiu: o oră
Obiective:

După citirea materialului, cititorul va înțelege conceptul de cloud computing așa cum este perceput în tehnologia IT și principalele servicii pe care acesta le include. De asemenea, veți cunoaște principalele avantaje și dezavantaje ale tehnologiilor cloud computing.

Realizări:

După studiul acestui material, vei putea să:

- cunoşti istoria termenului cloud computing;
- înţelegi semnificaţia termenului de cloud computing;
- cunoşti serviciile oferite de tehnologiile cloud;
- cunoşti avantajele şi dezavantajele tehnologiilor cloud.

Începând cu prima revoluţie industrială societatea umană pe ansamblul său a evoluat iar progresele ştiinţifice s-au ţinut lanţ. Omenirea a parcurs pe rând trei revoluţii industriale fiecare având propriile caracteristici. Începutul mileniului trei este marcat de apariţia celei de a patra revoluţii industriale caracterizată prin utilizarea pe scară largă a roboţilor industriali, a inteligenţei artificiale și a tehnologiilor cloud computing.

Toate aceste lucruri aduc profunde transformări în activitatea și viaţa oamenilor. Dacă termenii de roboți și inteligență artificială sunt oarecum sugestivi și nu oferă multă ambiguitate, termenul de cloud computing pare să fie mai mult un jargon decât un termen tehnic. Și totuşi acest termen are o semnificație tehnică importantă pentru industria IT.

Termenul de cloud este în realitatea o metaforă a termenului internet. De altfel pictograma referitoare la internet este reprezentarea unui nor, și înseamnă tot ce este cuprins în tehnologia internet nevăzut de utilizator. Cu alte cuvinte pictograma vrea să exprime faptul că tot ceea ce aparține de internet este ascuns într-o nebuloasă pentru utilizatorul de internet.

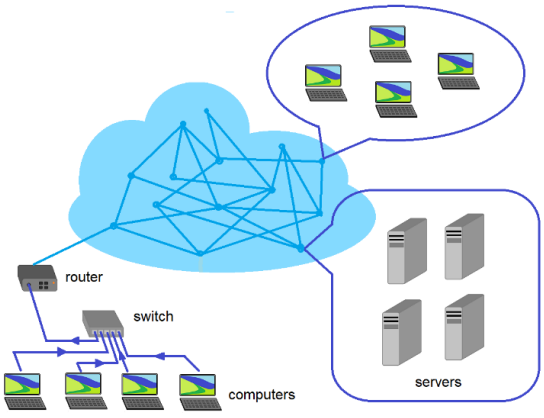

Figura 2.1. Imagine sugestivă a termenului de cloud computing

Tehnologiile cloud computing creează un impact deosebit asupra activităţilor economice din întreaga lume. Deşi înţelesul imediat al acestui termen ar fi serviciul de stocarea de date pe un server la o companie care deţine posibilitatea tehnică de stocare de date în condiţii de siguranţă, termenul complet al cloud computingului este mai larg. Îşi are originea la momentul în care au apărut sistemele de calcul.

Astfel după părerea majorităţii oamenilor de ştiinţă și a cercetătorilor conceptul de cloud computing ar fi fost enunţat într-o formă foarte simplă în anul 1955 când un om de ştiinţă din domeniul computerelor a venit cu ideea ca anumite resurse informatice să fie partajate între diverşi utilizatori prin închiriere, deoarece tehnologiile informatice de la acea vreme aveau costuri exorbitante iar mulţi utilizatori nu-și permiteau achizitionarea lor. Această idee aparține cercetatorului John McCarthy și este privită ca începutul conceptului de cloud computing.

Paisprezece ani mai târziu un alt cercetător, J.C.R. Licklider, a dezvoltat o reţea informatică locală în instituţia în care lucra care este considerată acum strămoşul internetului. Scopul reţelei lui Lickider avea rolul de a facilita schimbul de resurse informatice (programe soft și date) între cercetatorii din instituţia respectivă. Concepţia lui McCArthy de a închiria resurse informatice și reţeaua realizată de J.C. R. Licklider pentru schimbul de resurse IT au dus la dezvoltarea a ceea ce numim azi internetul. Iniţial acesta se numea Eternet.

În 1972 compania IBM a realizat primul calculator mainframe VM/370 sau Virtual Machine Faciltiy/370. Orice cercetător sau om de ştiinţă putea să acceseze datele stocate pe acest sistem utilizând un program de emulare Hercules. Dacă până în anii 80 ai secolului trecut tehnologiile informatice erau accesibile doar oamenilor de ştiinţă, cercetatorilor sau companiilor mari, în perioada 1980-1989 au apărut home computers și s-au îmbunătăţit tehnologille prin care se realizau reţelele de comunicare între computere. Reţeaua de comunicare s-a numit Eternet și a fost standardizată. Unele companii ca Ms_Dos și Novel au adus o contribuţie importantă în perfecţionarea reţelelor de comunicare între calculatoare. Resursele informatice erau găzduite pe servere care puteau fi accesate din orice loc și de oricine avea un sistem de calcul conectat la reţeaua de calculatoare.

Internetul a crescut exponenţial între anii 1990-1998. În 1996 un grup de cercetători ai companiei Compaq Computer au introdus pentru prima dată conceptul de cloud computing. Lansarea aplicaţiei SalesForce.com în 1999 a făcut posibilă vânzarea de informaţii unor compani colaboratoare sau posibilitatea de stocare prin intermediul unui portal web. Acesta a fost începutul unei perioade în care și alte companii au început să ofere aceleaşi servicii și au contribuit la îmbunătăţirea internetului. Apariţia pe piaţa produselor informatice a Serviciilor de Web oferite de compania Amazon a fost un moment important. Acest serviciu a oferit stocare de date, acces la programe și virtualizare.

Între anii 2006 și 2012 compania Google și-a consolidat prezenţa pe piaţa serviciilor de internet lansând Google Apps. În 2011 compania Apple a anunţat lansarea propriei soluţii de stocare a datelor pe servere accesate prin internet sub numele Apple iCloud. Un an mai târziu a fost lansată aplicaţia Google Drive de către compania Google care a unit toate facilităţile oferite sub un singur serviciu.

Între 2012-2017 serviciile cloud au fost extinse și datorită apariţiei dispozitivelor mobile performante astfel serviciile de cloud au fost accesate de tot mai mulţi utilizatori ceea ce a stimulat companiile IT să perfecţioneze serviciile oferite. Cercetarea în domeniul IT a dus și la creşterea nivelului tehnic al reţelelor pentru transferul datelor și astfel a crescut și viteza internetului.

Astazi, termenul de cloud este utilizat din ce în ce mai mult fără să se cunoască adevărata sa semnificație în tehnologiile informatice. Cea mai simplă definiție a termenului cloud computing este accea de a avea acces uşor la resurse informatice (programe și date) sau la alte servicii care nu sunt instalate pe calculatorul propriu. Pentru consumatorul casnic serviciile de cloud pot să însemne accesul la sevicii de poştă electronică, stocarea unor date în Google Drive sau utilizarea unor servicii specializate pentru trasferul fişierelor de dimensiuni mari imposibil de transmis prin email (ex. Drop Box). Poate să însemneze și accesare de filme, muzică sau jocuri prin internet.

Din punct de vedere al unor întreprinderi mici și mijlocii serviciile de cloud computing pot fi definite prin stocarea sigură a aplicaţiilor soft și datelor proprii în locaţii situate în afara companiei care să poată fi accesate uşor de oriunde și de către oricine este autorizat de conducerea companiei. Acest lucru aduce companiei beneficii financiare însemnate deoarece nu este necesar ca aceasta să achizitioneze echipamente proprii pentru stocarea datelor sau aplicaţiilor soft și nici nu este necesară prezenta unor specialiști pentru gestionarea activităţilor specifice IT.

Pentru a înlătura ambiguitățile în definiția termenului de cloud computing, Institutul Național de Standarde și Tehnologie din SUA (NIST) a definit serviciile de cloud computing în 2011 după cum urmează:
„Cloud computing este un model pentru a permite de peste tot, in mod convenabil si la cerere accesul la rețea a unui fond comun de resurse configurabile de calcul (de exemplu, rețele, servere, stocare, aplicații și servicii). Poate fi furnizat și lansat rapid cu un efort minim de management sau cu interacțiunea cu furnizorul de servicii”.

NIST a precizat și cinci caracteristici esenţiale pe care trebuie să le aibă cloud computingul:

- autoservire la cerere;
- acces larg la reţea;
- punerea în comun a resurselor;
- elasticitate sau expansiune rapidă;

- serviciu contorizat (măsurat).

Serviciile de cloud computing pot să fie furnizate de o companie care lucrează în domeniul IT sau pot fi accesate de o companie cu profil diferit de IT, de persoane fizice sau de comunităţi.
De aceea NIST a definit și patru tipuri de cloud computing:

- public;
- privat;
- comunitar;
- hibrid.

Fiecare din cele patru tipuri de cloud computing precizate mai sus poate să ofere următoarele servicii de bază:

1. software, (Software As A Service) – (SAAS);
2. platformă (Platform As A Service) – (PAAS);
3. infrastructură (Infrastructure As A Service) – (IAAS);

În cadrul unui serviciu de cloud computing care furnizează toate cele trei servicii de bază enumerate mai sus, ele sunt structurate după cum se arată în imaginea următoare (vezi Figura 2.2. de mai jos):

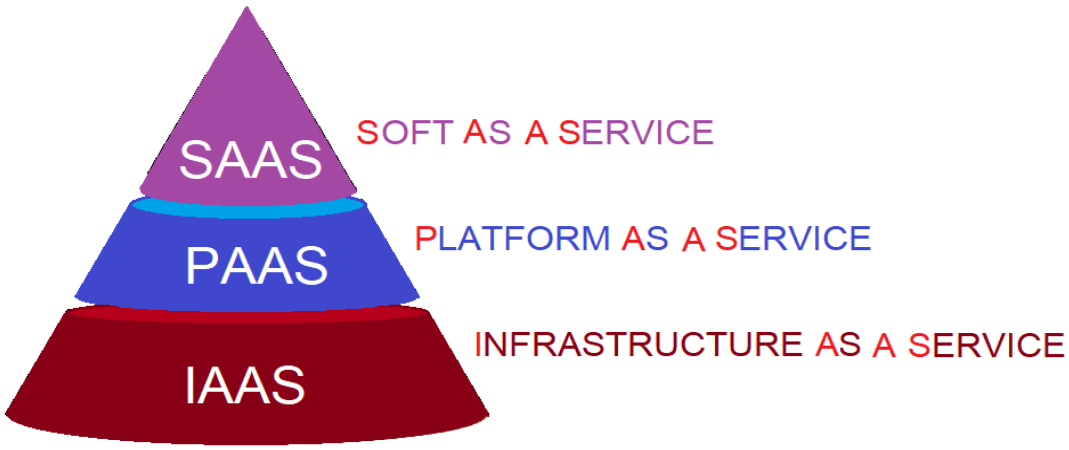

Figura 2.2. Ierarhia celor trei nivele de bază în serviciile de cloud computing

În afara celor trei servicii arătate până acum, companiile IT furnizează și alte servicii care au următoarele denumiri și acronime:

4 Gaming As A Service (GAAS).
5 Comunications As A Service (CAAS).
6 Database As A Service (DBAAS).
7 Desktop As A Service (DAAS).

8 Hardware As A Service (HAAS).
9 Identity As A Service (IDAAS).
10 Storage As A Service (STAAS).

În cele ce urmează vom explica definiția fiecărui serviciu:

- Software As A Service (SAAS) constă în furnizarea unor servicii cum ar fi: Gmail, Youtube sau alte servicii similare către utilizator. Prin utilizarea acestor servicii uneori se plăteşte o taxă de acces sau sunt gratuite.
- Platform As A Service (PAAS) oferă dezvoltatorilor de softuri o platformă pentru scrierea de coduri pentru diferite aplicaţii și de a le testa pe respectiva platformă.
- Infrastructure As A Service (IAAS) este un serviciu care constă în subînchirierea de servere și reţele unei companii care poate la rândul ei să le ofere ca servicii altor utilizatori.
- Gaming As A Service (GAAS) este un serviciu furnizat de unele companii prin care utilizatorii pot accesa softuri care oferă jocuri de amuzament în mediul virtual. Aceste softuri pot să ruleze pe calculatoare sau dispozitive mobile.
- Comunications As A Service (CAAS) sunt servicii de de mesagerie, videoconferinţe pentru comunităţi ai căror membrii nu se găsesc în același loc sau de comunicaţii la distanță prin voce sau text. În această categorie intră aplicaţii ca cele oferite de Skype , Facebook sau Twitter.
- Database As A Service (DBAAS) înseamnă furnizarea de servicii de baze de date care presupun stocarea datelor aparținând unor companii, comunităţi sau persoane pe serverele unor companii IT specializate în acest sens. Aceste date pot fi uşor și în siguranţă accesate de către proprietarul datelor. Proprietarul datelor plăteşte o taxă de închiriere pentru acest serviciu. Serviciul este rentabil deoarece crearea și administrarea unei baze de date specializată pentru un anumit domeniu presupune un efort financiar deosebit pentru multe companii.
- Desktop As A Service (DAAS) este un serviciu prin care o persoană oarecare poate utiliza calculatorul propriu prin accesarea acestuia de pe un alt dispozitiv când se află într-o altă locaţie. Procesul se numeşte virtualizare și permite accesarea unui calculator sub sistemele de operare Windows, Mac sau Linux prin intermediul tehnologiilor cloud, utilizând pictogramele, scurtăturile etc. ale calculatorului accesat.
- Hardware As A Service (HAAS) permite unei companii să închirieze elemente hardware de la un furnizor. Toate elementele hardware: computere, imprimante, telefoane mobile, tablete etc. sunt în proprietatea furnizorului pe timpul în care sunt utilizate de compania care le-a inchiriat. Acest serviciu este considerat că face parte din tehnologia cloud deşi pare diferit de celelalte servicii specifice tehnologiei.
- Identity As A Service (IDAAS) asigură accesul securizat la resursele informatice prin softuri care identifică amprenta digitala sau detecţia irisului ocular a celui care doreşte accesul la date. Pe lângă aceste elemente utilizate la detecţie pot există și alte procedee pentru verificarea identităţii celui care solicită accesul la datele stocate.

- Storage As A Service (STAAS). Google drive și Dropbox sunt două exemple ale acestui tip de serviciu. În principiu prin acest serviciu se permite stocarea unor date aparținând angajaților unei companii sau a unor persoane fizice. Aceste date pot fi oricând accesate de proprietarul lor garantându-se securitatea datelor.

După cum s-a menționat mai sus, termenul de cloud este considerat o metaforă a internetului. De-a lungul timpului pe lângă serviciile de comunicare între calculatoare cunoscute sub numele de Internet, (care presupuneau existenta unei rețele și a unor softuri specializate),
s-au creeat de către companii mai multe facilități care au devenit ulterior servicii. Termenul de cloud se poate referi la rețele locale de internet ale unor companii care furnizează servicii în domeniul IT într-o zonă geografica sau la întreaga rețea internet răspândită pe întreg mapamondul. Ca urmare se poate vorbi despre un cloud local și un cloud general. Pe piața mondială există patru companii gigant care oferă servicii de cloud computing. Acestea sunt: Microsoft cu serviciul Microsoft OneDrive, Amazon care oferă serviciul Cloud Services, Apple oferă serviciu iCloud și Google care oferă servicii de Gmail, Drive etc. Pe lângă acestea sunt serviciile Dropbox Cloud services.

O companie IT oarecare poate să opteze să-și realizeze propriul sistem de cloud local pe care să-l închirieze unor utilizatori finali care pot fi persoane fizice, comunități locale sau companii cu profil de activitate diferit de IT.

Un sistem pentru cloud computing este alcătuit din:

- Rețeaua locală de Internet a unuia sau mai multor utilizatori. Toate computerele, imprimantele și celelalte componente hardware ale unui utilizator sunt conectate la unul sau mai multe switch-uri locale.
- Switch-ul utilizatorului este conectat la un router care se conectează la rețeaua locală sau la rețeaua Internet a unui furnizor de servicii internet ISP (Internet Service Provider).
- Conectarea la un serviciu de cloud se face printr-un portal sau un website al unei companii care dispune de propriile rețele locale și servere. În serverele companiei de cloud pot fi stocate date sau să fie rulate aplicații soft. Comunicarea între serverele companiei și utilizator se face printr-un portal frontend. Toate serverele companiei de cloud sunt interconectate între ele și formează un cluster. Clusterele de servere pot fi localizate oriunde în lume și pot fi situate în locuri diferite la distanțe mari unele de altele.

Compania proprietară a clusterelor de servere asigură accesul securizat al utilizatorilor, întreține baza de date și actualizează programele soft oferite clienților. O definiție mai simplă a unui serviciu cloud este un centru de date în care sunt interconectate sute de servere care oferă posibilități de stocare și de rulare a unor softuri la care au acces companii sau persoane fizice gratuit sau plătit. Pe lângă

posibilitatea de stocare a datelor sau de rulare a unor softuri aplicative serviciile de cloud mai pot oferi și unele dintre serviciile enumerate mai sus.

Figura 2.3. Aspecte din interiorul unui centru de date care oferă servicii de cloud computing

Utilizarea serviciilor de cloud computing oferite de o companie IT are următoarele avantaje:

✓ Acces uşor din orice loc din lume. Datele stocate pe server pot fi accesate de oriunde din lume de către persoana proprietară a datelor. Condiţia este ca persoana să poată avea acces la internet și să posede un dispozitiv prin care să poată avea acces la internet

✓ Reducerea costurilor companiei – deoarece compania nu este nevoită să investească în achiziţionarea de echipamente hardware și să angajeze specialiști în IT pentru realizarea softurilor și pentru administrarea bazelor de date. De multe ori investiţiile în echipamente hardware și software sunt mai mari decât beneficiile pe care o companie cu alt profil de activitate le realizează de pe urma lor.

✓ Flexibilitatea – caracterizează faptul că pot fi schimbate cu ușurință caracteristicile softurilor sau a interfeţelor utilizator după dorinţa clientului. Acest lucru poate duce la realizarea unor performanțe în afaceri.

✓ Actualizare permanentă a tehnologiilor IT. Tehnologiile IT referitoare la bazele de date dar și la softurile utilizate pentru transferul bazelor de date sunt într-un continuu progres. Furnizorii de servicii de cloud computing achiziţionează noile tehnologii astfel încât să ţină pasul cu progresul tehnic. Astfel utilizatorul de servicii cloud poate beneficia de ultimele noutăţi în domeniul acestor tehnologii.

✓ Protecţia datelor la dezastrele naturale care ar afecta compania proprietară. Datele și aplicatiile soft utilizate de o companie sau o comunitate pot fi pierdute în cazul în care un incendiu sau un sau dezastru natural ar afecta compania proprietară a datelor în cazul în care acestea sunt stocate pe servere sau pe alte dispozitive locale. Deoarece datele companiei sunt stocate pe servere situate la distanță de compania proprietară, datele acesteia sunt în siguranţă.

✓ Colaborarea între angajaţii unei companii sau a mai multor companii prin accesul la programe sau date. Angajaţii unei companii care colaborează la un proiect pot să acceseze uşor aceleaşi date care sunt stocate pe server mult mai uşor.

✓ **Securitatea datelor.** Accesul la datele sau programele stocate pe serverele unei companii IT este securizat și se face pe baza unor parole de acces. Dacă datele stocate pe server ar fi ţinute pe un sistem de stocare local, CD-rom, stick sau chiar într-un laptop pierderea sau furtul acestuia duce la pierderea iremediabilă a datelor. De asemenea compania care oferă serviciile de cloud ia măsuri stricte pentru a opri accesul persoanelor neautorizate la datele stocate.

Deşi serviciile de cloud computing au avantaje care le recomandă să fie utilizate pe scară largă totuşi aceste servicii au și unele dezavantaje. Aceste dezavantaje sunt:

- Actualizarea softurilor care gestioneaza funcţionarea serverelor poate duce la pierderea datelor stocate. Un exemplu este cel din anul 2011 când compania Amazon a pierdut datele clienţilor săi.
- Lipsa legăturii la internet este un dezavantaj major, pentru persoana care se găsește
- într-un loc unde nu are acces la internet deoarece nu poate utiliza datele din server.
- În cazul unor companii care oferă servicii cloud cheltuielile pot creşte și să oblige compania să suspende serviciile oferite clienţilor.
- Incapacitate de a accesa serverul unei companii chiar dacă legătura la internet este posibilă. S-a întâmplat în trecut chiar la companii de renume în care a apărut mesajul **HTTP Error 503 The server is unavailable**. Din fericire acest lucru se întâmplă rar.
- Accesul guvernelor la datele personale sau ale companiilor. Guvernele pot forța companiile de cloud computing să le ofere accesul la datele stocate pe serverele lor în scopul de a obține informaţii confidenţiale despre cetăţenii sau despre companiile care au stocate date pe serverele respective. Pentru a menţine secretul datelor stocate, unele companii și-au mutat serverele pe teritoriile altor state și astfel ies de sub jurisdicţia statului care solicită accesul la datele stocate pe serverele lor.
- Serverele pot fi atacate de hackeri. În acest caz securitatea datelor este în pericol. Au fost situaţii în care persoane celebre au reclamat că le-au fost furate date personale stocate pe serverele unor companii de cloud.

În ciuda tuturor dezavantajelor enumerate mai sus serviciile de cloud computing sunt din ce în ce mai utilizate în întreaga lume și foarte multe companii din domeniul IT investesc pentru creşterea calităţii serviciilor de cloud computing.

2.2 Compararea preţurilor de piaţă între AWS, Azure și GCP (Google Cloud Platform).

Nivel de dificultate: uşor
Perioada de studiu: 45 minute per unitate, 4 unităţi în Module
Obiective:

Cloud computing este unul dintre cele mai populare cuvinte la modă din industria IT în acest moment, deoarece furnizorii de cloud oferă peste tot avantajele unei configurații ușoare, scalabilitate ridicată și accesibilitate.

Următoarele unități din acest modul vă vor familiariza cu cei mai buni furnizori de cloud disponibili astăzi pe piață. Amazon Web Services (AWS), Google (GCP) și Microsoft (Azure) sunt cei mai cunoscuți furnizori publici de cloud și dețin o cotă de piață de miliarde de dolari în cloud computing.

Pe măsură ce progresăm prin unitățile de învăţare, vom trece de la o prezentare generală a acestor 3 furnizori la o analiză concentrată asupra a ceea ce oferă aceștia la preț. Este o realitate comună că soluțiile de ultimă oră în cloud vin cu un preț, care nu este diferit pentru acești trei mari furnizori — AWS, Azure și Google — deoarece vom analiza modul în care prețurile lor variază în funcție de planurile lor, de selecția de servicii, de caracteristici, opțiuni de reducere, utilizarea resurselor și multe altele.

Realizări:

După finalizarea acestui modul, veți putea să:

- înțelegeți cererea pentru platforme de cloud computing;
- recunoaşteţi influența lor în sectorul managementului afacerilor, printre altele;
- recunoașteți unele dintre asemănările și diferențele dintre platformele cloud din perspectivă tehnică;
- aflați despre prezența pe piață a celor 3 platforme, o comparație între ele;
- aflați cum sunt stabilite opțiunile de preț și cum sunt legate de cererea pieței după 2019.

2.2.1 Ce oferă cloud computing-ul

De ce ați apela la o platformă cloud pentru nevoile dvs.? Această unitate analizează ceea ce oferă cloud computing pentru cineva ca dvs., care speră să gestioneze o afacere sau caută orice tip de asistență IT

Să vorbim despre elementele de bază

Aceste platforme sunt similare în ceea ce privește factorii cheie, de ce domină piața deşi fiecare oferă resurse diferite când vine vorba de opțiuni de calcul, rețea și stocare.

Este clar că atunci când căutați cea mai bună platformă de cloud computing pentru afacerea dvs., este important să vă urmăriți obiectivele, creșterea așteptată și bugetul.

Ce oferă cloud computing?

Să ne uităm la câteva dintre principalele motive pentru care cloud computing este excelent pentru ceea ce aveți nevoie atunci când vă ajutați în gestionarea unei afaceri:

- Costuri IT reduse: Implementările în cloud vă permit să plătiți numai pentru capacitatea de calcul în funcție de nevoile dvs. de afaceri, reducând costurile continue de achiziție, implementare, întreținere și gestionare a infrastructurii locale.
- Timp mai rapid de introducere pe piață: cloud-ul este activat în câteva minute. Fără timpi de așteptare pentru a începe.
- Scalabilitate și flexibilitate ridicate: Implementările în cloud pot scala automat sarcinile de lucru ca răspuns la cerințele pieței în schimbare.
- Îmbunătățirea fiabilității afacerii: Implementarea backup-ului datelor și a recuperării în caz de dezastru în cloud este, de obicei, mult mai ușoară, mai puțin costisitoare și mai puțin perturbatoare decât la locația proprie, (la locaţia proprie este riscant și consuma mult timp).
- Îmbunătățiri continue de performanță: Deoarece este în timp real, infrastructura cloud este actualizată în mod regulat cu cel mai recent și mai puternic hardware de calcul, de stocare și de rețea.
- Asigurați-vă măsuri de securitate: îndepliniți cu ușurință cerințele de bază de securitate și conformitate cu cel mai flexibil și mai sigur mediu cloud disponibil în prezent.
- Imaginea de mai jos (Figura 2.4.) arată cum utilizarea cloud-ului reduce costul general al IT în gestionarea unei afaceri și de ce este atât de atrăgător pentru utilizatori:

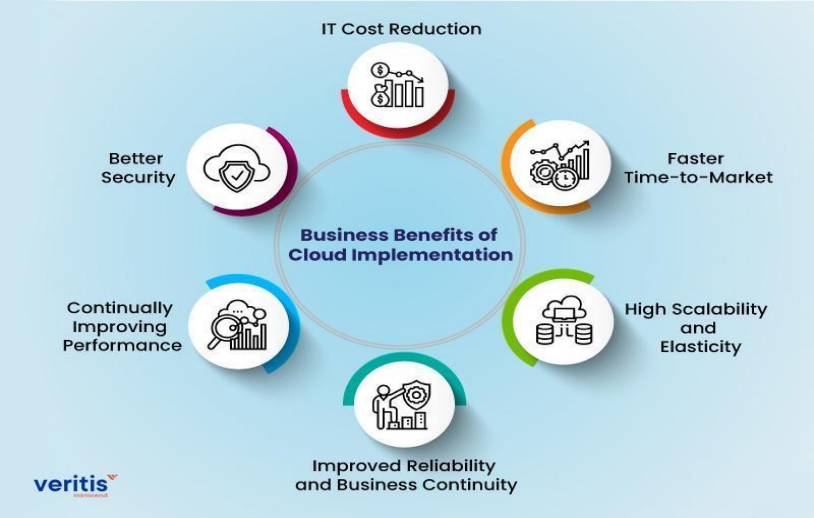

Figura 2.4. Beneficiile implementării cloud-ului pentru afaceri

Iată câteva definiții de bază ale celor trei furnizori:

Ce este AWS Cloud Platform?

AWS, sau Amazon Web Services, este o platformă de servicii cloud de la Amazon care oferă utilizatorilor servicii de calcul, stocare, livrare și alte servicii. Luate împreună, toate aceste oferte Software-as-a-

Service (SaaS), Infrastructure-as-a-Service (IaaS) și Platform-as-a-Service (PaaS) pot fi utilizate în mod eficient de dvs., deoarece oferă următoarele caracteristici:

- Peste 18.000 de servicii.
- Calculatoare.
- Soluţii de depozitare.
- Integrarea aplicației în cloud.
- Analiză și învățare automată.
- Instrumente de productivitate.
- Dezvoltator și instrumente de management.

Amazon Web Services este cel mai popular serviciu de stocare pentru arhivele de obiecte, motiv pentru care domină actuala piață cloud. Aceasta constă din instrumente pentru IoT, securitate, baze de date, management, analiză, aplicații pentru întreprinderi și multe altele.

De la Amazon vin trei niveluri separate de asistență pentru dezvoltatori, asistență pentru afaceri și asistență pentru întreprinderi, oferind o combinație de instrumente, tehnologie cloud și experți.

Multe dintre punctele forte ale AWS sunt legate de poziția sa de furnizor principal de servicii cloud moderne și de amploarea operațiunilor sale globale. Luați împreună, acești factori au alimentat creșterea AWS și i-au permis companiei să ofere o listă mare de servicii non-stop companiilor din întreaga lume.

Iată câteva dintre punctele forte ale AWS:

- Acceptă toate sistemele de operare majore, inclusiv macOS (spre deosebire de alți furnizori).
- Oferă o gamă largă de servicii.
- Creșterea continuă a ofertelor de servicii.
- Sofisticat și ușor disponibil.
- Poate gestiona un număr mare de utilizatori finali și resurse.
- Foarte ușor de accesat și de pornit.

Iată câteva dintre dezavantaje:

- Un cost relativ ridicat.
- Taxe suplimentare pentru serviciile esențiale.
- Cost suplimentar pentru suport tehnic pentru clienți.
- Curbă abruptă de învățare după accesarea platformei.

Microsoft Azure

Deoarece există și o platformă integrată pe cloud care oferă stocare, aceleași oportunități de baze de date și calculatoare pe care le are Amazon, are și diferite tipuri de cloud care răspund cerințelor

specifice. Este una dintre cele mai bune opțiuni din cloud pentru companiile care au nevoie de o cantitate mare de spațiu de stocare a datelor, cu opțiuni precum Data Lake Storage și Queue Storage. Stocarea în vrac este ideală pentru companiile cu o cantitate mare de date nestructurate, în timp ce stocarea fișierelor este ideală pentru companiile cu cerințe specifice de stocare a fișierelor. Azure se bazează pe software-ul actual al setului de birou Microsoft, alte instrumente de afaceri pentru a oferi următoarele caracteristici, într-un format configurat:

- O platformă de dezvoltare pe cloud.
- Tehnologia blockchain.
- Software predictiv.
- Instrumente de integrare IoT.

Google Cloud Platform (GCP)

O caracteristică importantă a Azure, la fel ca Amazon, este abordarea pe niveluri a serviciilor de asistență, care include un plan pentru dezvoltatori care oferă suport nelimitat în timpul orelor de lucru și planul standard, care include și acces nelimitat. Pentru un suport mai structurat pentru afaceri, planul profesional pentru cloud este cea mai bună opțiune.

Utilizatorii se bucură de caracteristicile speciale ale Azure datorită:

- Disponibilității pe scară largă.
- Bonurilor de contract de servicii pentru utilizatorii de cloud computing Microsoft.
- Configurării intuitive cu familia de software Microsoft.
- Aplicațiilor încorporate care acceptă mai multe limbaje (inclusiv Java, Python, .NET și PHP).

Unele dintre problemele care pot fi întâlnite includ:

- Gestionarea inadecvată a datelor.
- Rapoarte privind dificultățile de bază ale rețelei.
- Unii oameni cred că este mai dificil de stăpânit decât alte platforme.
- Designul poate părea mai puțin profesional decât pe alte platforme.
- Probleme raportate de asistența tehnică.

Google Cloud Platform (GCP)

Datorită expertizei sale IT nesfârșite și cercetării interne, Google s-a dovedit a fi un competitor pe piață. Dispune de multe servicii găzduite, cum ar fi Platform as a Service (PaaS) și Infrastructure as a Service (IaaS) pentru calcul, stocare și dezvoltare de aplicații.

Google a fost făcut public pentru prima dată în 2004, dar a început abia recent să reprezinte o amenințare serioasă atât pentru AWS, cât și pentru Azure.

GCP recuperează rapid concurența datorită prezenței globale extinse a Google și capacității aparent nelimitate de inovare.

În prezent, oferă servicii precum:

- gestionarea productivității în afaceri și în alte domenii;
- stocarea datelor;
- studio de dezvoltare de aplicații în cloud;
- motoare pentru AI și învățare automată, cum ar fi API-ul de vorbire în cloud, API-ul de viziune și altele;
- analiza de afaceri și alte componente suplimentare.

Spre deosebire de celelalte două servicii, opțiunile de stocare ale Google sunt destul de simple, cu stocarea în cloud și stocarea persistentă pe disc care completează lista. Pe lângă propriul serviciu de transfer intern, Google oferă utilizatorilor și acces la un număr tot mai mare de servicii de transfer online. Din păcate, opțiunile de rezervă ale Google - backup Nearline pentru datele accesate frecvent și backup Coldline pentru datele accesate rar – sunt si ele mai degrabă servicii de bază.

Câteva caracteristici remarcabile oferite de GCP includ:

- grad ridicat de scalabilitate;
- configurare și instalare simplă;
- utilizarea limbajelor de programare utilizate pe scară largă precum Python și Java;
- economii rezonabile pe termen lung;
- echilibrarea încărcării datelor și răspunsuri rapide.

Dezavantajele includ următoarele:

- Caracteristici avansate inadecvate.
- Mai puține variații ale caracteristicilor.
- Mai puține opțiuni de service.
- Există puține centre de date globale.

Întrebări de luat în considerare

1. Ce este o platformă cloud și ce avantaje oferă?
2. Numiți 3 dintre beneficiile afacerii din cloud din grafic și de ce vă atrag.
3. Pe cine ați alege ca furnizor și de ce?

Verificați sursa, intitulată Techfunnel (2022) și răspundeți din ceea ce ați învățat

2.2.2 Cei trei jucători cheie de pe piață

Trei furnizori de servicii cloud importanţi controlează cea mai mare parte a pieței, reprezentând 64% din cota totală de piață. După cum se vede în graficul de mai jos, AWS deține primul loc cu o cotă de piață de 33%, urmat îndeaproape de Azure cu 21% și Google Cloud cu 10%, așa cum se vede în graficul de mai jos (Figura 2.5.).

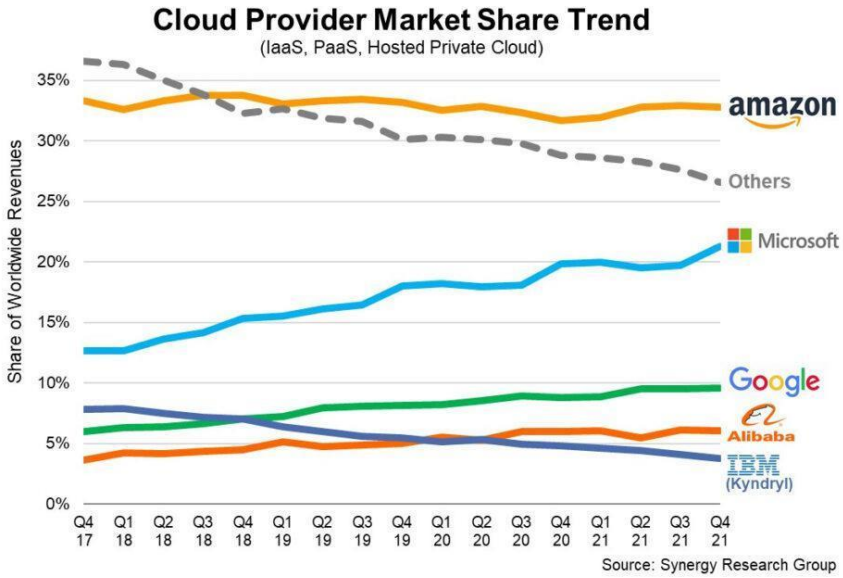

Figura 2.5. Tendința cotei de piață a furnizorilor de cloud

Datorită rețelei globale extinse a acestor furnizori de cloud, aceste cifre pot fi explicate.

Cu o piață care devine din ce în ce mai mare, Amazon este un caz interesant, deoarece cota sa de piață s-a stabilizat la aproximativ 33%. Cu alte cuvinte, în ultimii ani, veniturile din cloud ale AWS au crescut in mod constant. Deși concurența este din ce în ce mai puternică, AWS își vinde produsele cloud de 11 ani și continuă să fie lider de piață. Alții imită ceea ce face Amazon atunci când adoptă o nouă tehnologie sau strategie de afaceri.

Potrivit lui Jeff Bezos, CEO al AWS, „AWS a avut avantajul neobișnuit al unui avans de șapte ani înainte de a se confrunta cu o concurență similară". Din acest motiv, serviciile AWS sunt de departe cele mai avansate și funcționale. AWS a raportat un venit de 62 de miliarde de dolari și un profit net de 18,5 miliarde de dolari în 2021. În comparație cu cifra de afaceri de anul trecut, aceasta reprezintă o creștere de 38%.

Dar aici este şiretlicul. Microsoft este, fără îndoială, cel mai mare competitor al AWS; Divizia Intelligent Cloud a Microsoft a generat anul trecut venituri de 60 de miliarde de dolari, ceea ce este foarte aproape de veniturile AWS, deci iată care este câştigul: această divizie include și multe alte servicii, inclusiv

Microsoft Azure, GitHub, Windows Server, Microsoft SQL Server și alte versiuni ale acestor produse. Veniturile diviziei pentru inteligenţa cloud au crescut cu 24% din 2020 până în 2021.
Google Cloud este al treilea cel mai mare furnizor de cloud după AWS și Azure.

Veniturile sale au crescut de la 13 miliarde USD în 2020 la 19 miliarde USD în 2021. Pierderea operațională Google Cloud a scăzut cu 2,5 miliarde USD din 2020 până în 2021. Scăderea pierderii operaționale a fost determinată în principal de creșterea veniturilor.

La fel ca Microsoft Azure, divizia de cloud Google încorporează și feedback din alte locuri, cum ar fi spațiul de lucru Google. În anii precedenți, Google Cloud a făcut investiții semnificative, care au dus la pierderi de exploatare, pentru a ajunge din urmă pe AWS și Azure. La începutul acestui an, Ruth Porat, CFO Google și Alphabet, a prezis acest lucru în următorul mod: „În viitor, ne vom concentra în continuare pe creșterea veniturilor determinată de investițiile continue în produse și organizarea de lansare pe piață. Gama va reduce în cele din urmă pierderile din exploatare și va îmbunătăți marja operațională."

Iată o privire rapidă asupra unor aspecte cheie ale fiecăruia:
Azure Virtual Network: Azure este în prezent accesibil în 54 de regiuni din întreaga lume și păstrează cât mai mult trafic posibil în interiorul rețelei Azure, mai degrabă decât prin internet. În cele din urmă, este o soluție de rețea care funcționează mai bine decât AWS este rapid și sigur. În plus, deoarece rețeaua virtuală Azure este atât de flexibilă, companiile pot utiliza o strategie de rețea hibridă sau pot aduce propriile adrese IP și servere DNS.

Amazon Direct Connect: Pentru a garanta un serviciu constant și performanță de încredere în orice moment, Amazon a creat un cadru global cuprinzător, centrat pe 114 locații marginale, 14 centre de date și 22 de regiuni globale diferite. Drept urmare, AWS este capabil să ofere modele de implementare rapidă în cloud, livrare rapidă și timpi de răspuns instantaneu pentru gama sa largă de servicii. În special, VLAN-urile 802.1q, care sunt standarde din industrie, permit o conexiune dedicată între rețelele private și AWS prin oricare dintre numeroasele locații de conectare directă.

GCP: În ciuda faptului că nu au același domeniu de aplicare ca ceilalți doi furnizori, renumitele capabilități de inovare ale Google acceptă Google Cloud Platform. Pe lângă un număr mare de centre de date situate în întreaga lume, Google are în prezent 21 de regiuni și adaugă continuu mai multe prin adăugarea cablurilor submarine. Produsele de conectivitate hibridă precum Cloud Interconnect și Cloud VPN vă permit să stabiliți conexiuni directe sigure sau conexiuni VPN IPsec.

Pentru a înțelege cota de piață în cloud pentru fiecare dintre cei trei furnizori majori, ar trebui să fiți familiarizat, de asemenea, cu cifrele actuale ale cotelor fiecărei companii:

AWS: Cu o cotă de piață de 32%, Amazon conduce piața globală. De fapt, a depășit celelalte două cele mai populare platforme cloud din punct de vedere al veniturilor, aducând un respectabil venit de 11,6 miliarde de dolari și înregistrând o rată de creștere de 29% în acest trimestru.

Azure: Cu Azure, care deține o cotă de piață de 19%, Microsoft are o cotă de piață considerabilă. Microsoft a raportat o rată de creștere de 48% față de trimestrul precedent, în ciuda faptului că nu dezvăluie public cifrele de venituri ale Azure.

Google Cloud Platform: GCP se extinde în continuare rapid și se află în prezent pe locul trei, cu o cotă de piață de 7%. Creșterea sa este de fapt de 45% de la an la an, cu un venit total de 3,44 miliarde USD în acest trimestru.

În 2022, piața cloud va doborâ toate recordurile anterioare. AWS, Azure și GCP vor concura pentru cota de piață.

În urma pandemiei care a accelerat adoptarea cloud computing-ului în ultimii doi ani, putem observa că cifrele continuă să crească și că criza a fost mai mult un impuls pe termen lung pentru piața cloud decât un efect pe termen scurt.

S-a remarcat recent că companiile care au adoptat cloud computing-ul în ultimii ani și-au crescut utilizarea și acum se îndreaptă din ce în ce mai mult către strategii multicloud. Raportul Flexera State of the Cloud 2022 a arătat, de asemenea, că companiile investesc o sumă din ce în ce mai mare de bani în aceste tehnologii și ca rezultat, apar noi probleme precum securitatea, managementul multicloud și adoptarea Kubernetes. Deoarece mizele sunt întotdeauna mai mari, este esențial pentru companii să înțeleagă mai bine și să utilizeze resursele cât mai eficient posibil.

Companiile fac investiții semnificative la scară globală. Cheltuielile pentru cloud-urile publice vor crește de la 408 miliarde de dolari în 2021 la 474 de miliarde de dolari până la sfârșitul lui 2022, conform prognozei Gartner.

Întrebări de luat în considerare

- Care sunt procentele actuale ale cotei de piață în rândul furnizorilor?
- Luați în considerare diferențele dintre furnizori în ceea ce privește cota de piață în cloud.
- De ce ar crește sau scădea cota de piață: numiți câțiva factori și indicați care ar putea fi unele dintre previziunile dvs. viitoare pentru cei 3 furnizori.

2.2.3 Comparația cotei pentru piața cloud

Pentru a înțelege mai bine cum se mișcă piața la nivel global, să ne uităm la cotele de piață globale deținute de cei trei mari pe următoarele piețe majore: în Statele Unite, în Europa și în China.

Piaţa de cloud din SUA

Nu ar trebui să fie surprinzător că piața cloud din SUA, care reprezintă 44% din toate cheltuielile globale, este de departe cea mai mare. Primii trei furnizori de servicii cloud au în continuare aceeași cotă de piață: AWS are 37%, Azure are 23% și GCP are 9%. AWS, Azure și Google Cloud intenționează să deschidă noi centre de date în SUA în 2021. Microsoft Azure, de exemplu, a început să opereze în Georgia și Arizona în 2021, iar acest număr va continua să crească, deoarece au anunțat recent planuri de a construi de la 50 la 100 de noi centre de date în fiecare an în întreaga lume. Din figura de mai jos putem vedea costurile serviciilor de infrastructură cloud pentru timestrul 1, 2021 comparativ cu anii 2019 și 2020 (vezi Figura 2.6. – Q1, Q2, Q3, Q4 –trimestrul 1, trimestrul 2, trimestrul,3, trimestrul 4)

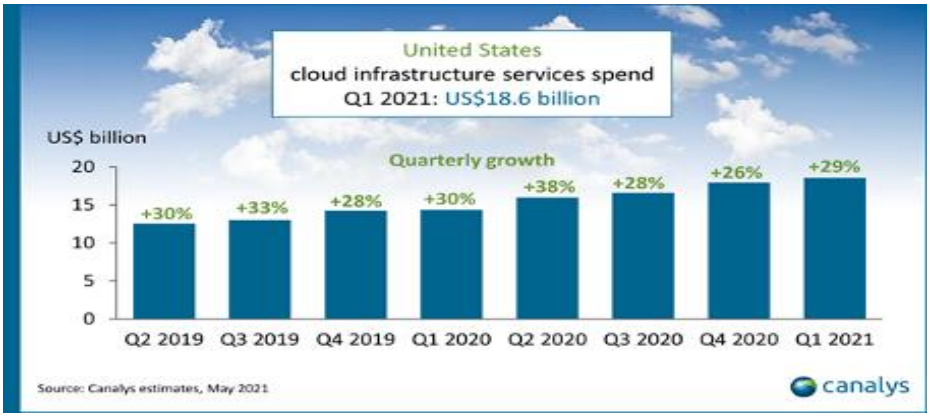

Figura 2.6. Costurile serviciilor de infrastructură cloud pentru trimestrul 1 (Q1) 2021 în SUA comparativ cu anii 2019 și 2020

Piața cloud din SUA este de departe cea mai mare și reprezintă 44% din cheltuielile totale, ceea ce nu este surprinzător. În graficul de mai sus, puteți vedea vârfuri semnificative de creștere (38%) în timpul crizei COVID și, mai recent, o creștere de 29% în trimestrul 1(Q1) 2021 pentru a atinge un record de 18,6 miliarde USD.

Piața cloud din Europa

Deși a crescut în timpul erei Covid, piața europeană de cloud este încă doar a treia ca mărime după SUA și China.

Furnizorii naționali de servicii cloud precum Deutsche Telekom, OVH, Scaleway, Orange și diverse companii de telecomunicații naționale sunt disponibili pe piața europeană. Acești furnizori concurează cu primii trei furnizori de servicii cloud din lume, AWS, Azure și GCP, care controlează acum 66% din piață, în creștere față de 50% în urmă cu trei ani.

Se anticipează că piața europeană de cloud va crește foarte puternic în următorii ani, noi centre de date apar pe tot continentul, în ciuda întârzierii sale în raport cu alte regiuni semnificative. Până în 2030, conform diferitelor proiecții, piața europeană va avea o valoare mai mare de 300 de miliarde de dolari, ceea ce ar fi egal cu dimensiunea pieței globale de astăzi.

Piața cloud din China

Piața cloud chineză crește în continuare cu o rată de două ori mai rapidă decât cea din SUA (60 față de 30%), depășind restul lumii. China a reprezentat 14% din piața globală de cloud în trimestrul 2 al 2021, cu cheltuieli pentru infrastructura cloud care au depășit 6 miliarde de dolari, așa cum se vede în graficul de mai jos (vezi Figura 2.7.).

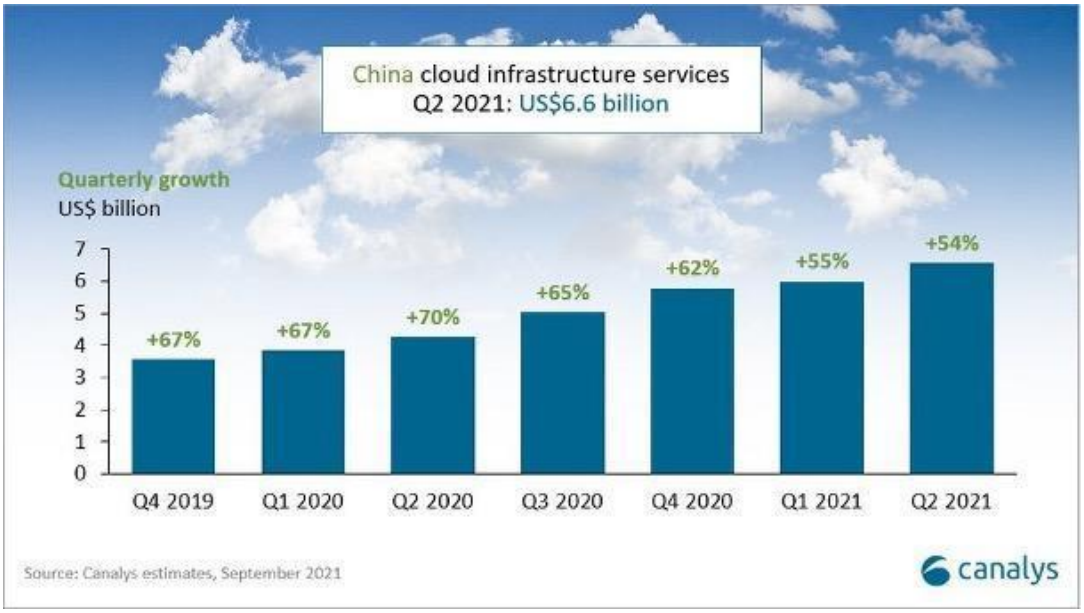

Figura 2.7. Costurile serviciilor de infrastructură cloud pentru trimestrul 1 (Q1) 2021 în China în comparație cu anii 2019 și 2020

Pandemia a accelerat creșterea în același mod în care a făcut-o în alte regiuni de piață; în trimestrul 2 al 2020, creșterea a atins un vârf de 70%. Există și alte motive care stau la baza acestei creșteri rapide: China este singura economie semnificativă care a raportat creștere economică pentru 2020, cu o creștere a PIB-ului de 2,6%. Guvernul chinez a făcut din cloud computing o prioritate de top prin strategia sa „Internet plus" în 2015.

Guvernul promovează și subvenționează industria cloud. Giganții tehnologici chinezi precum Alibaba, Tencent, Baidu, Huawei oferă soluții cloud și pot concura împotriva rivalilor lor americani, deoarece au o dimensiune echivalentă. Alibaba, Huawei Cloud, Tencent și Baidu AI Cloud, care împreună reprezintă mai mult de 80% din cheltuielile totale, sunt principalii furnizori de cloud pe piața cloud chineză. Companiile americane se luptă din cauza legilor care favorizează afacerile chineze.

Furnizorii chinezi de servicii cloud își propun acum să se dezvolte în Europa, Asia și țările în curs de dezvoltare. Putem anticipa o competiție digitală între SUA și China, similară rețelei 5G.

Întrebări de luat în considerare
1. Care sunt statisticile cheie ale pieței cloud din SUA?. Numiți două moduri prin care China poate spera să provoace piața SUA și preziceți dacă va avea succes în ambițiile sale?

2.2.4 Analiza structurilor de prețuri

Pentru a înțelege structurile de preț, este esențial să știți că fiecare dintre cele trei platforme principale are două lucruri în comun: un nivel gratuit cu foarte puține opțiuni și un model de preț la cerere la oră sau la minut pentru toate resursele. Compararea prețurilor poate fi o provocare, deoarece acestea pot diferi semnificativ în funcție de utilizarea resurselor, preferințele de servicii și alți factori.

În general, un război al prețurilor este se duce întotdeauna între primii trei: prin scăderea prețurilor, Microsoft și Google încearcă să provoace AWS. Utilizatorii serviciilor AWS plătesc numai pentru ceea ce folosesc, fără taxe suplimentare sau taxe de reziliere datorate după finalizarea serviciului. Acesta este cunoscut sub numele de model cu plata măsurată (contorizată) după consum (pay-as-you-go model).

Iată caracteristicile cheie ale modelelor de prețuri ale tuturor celor trei furnizori:

Prețuri pentru AWS. S-a afirmat că structura prețurilor oferită de Amazon este „atât de complexă, încât veți avea nevoie de o aplicație terță parte pentru a o gestiona”. Cu toate acestea, Amazon oferă o perioadă de 12 luni de 750 de ore pe lună de servicii EC2 ca parte a nivelului său gratuit, precum și o reducere de până la 75% pentru un angajament de 1-3 ani.

- cost ridicat în comparație;
- taxe suplimentare pentru serviciile necesare;
- taxele de asistență tehnică pentru clienți sunt taxate suplimentar.

Structura prețurilor din cadrul AWS este atât de complexă încât aveți nevoie de o aplicație terță parte pentru a gestiona toate aceste servicii. Instanța minimă, care are 2 procesoare virtuale și 8 GB RAM, vă

va costa aproximativ 69 USD pe lună, în timp ce instanța maximă, care are 128 procesoare virtuale și 3,84 TB RAM, vă va costa aproximativ 3,97 USD pe oră.

Tariful Azure. Utilizatorii Azure folosesc frecvent o aplicație terță parte pentru a gestiona costurile, deoarece este complexă într-un mod similar cu AWS. Similar cu AWS, Azure oferă un nivel gratuit care permite utilizatorilor să folosească 750 de ore de mașini virtuale pe lună timp de 12 luni în schimbul unei reduceri semnificative dacă se angajează pentru o perioadă de unu până la trei ani.

- Reduceri la contractele de servicii pentru utilizatorii serviciilor de cloud computing ale Microsoft.
- Prețuri accesibile la cerere.
- Utilizarea unor redundanțe mari pentru a reduce timpul de nefuncționare.

O serie de variabile, inclusiv locația, capacitatea necesară și nivelul de management, afectează prețul Azure. De asemenea, oferă un nivel gratuit, care permite utilizarea gratuită a anumitor modele numai pentru primele 12 luni, precum și utilizarea gratuită a anumitor modele pentru totdeauna.

Prețul cu plata măsurată după consum este o opțiune de la Azure, la fel ca și de la AWS. De asemenea, oferă o modalitate diferită de a plăti anticipat pentru serviciul său, la care se referă ca „Reserved Instance (Instanță Rezervată)" (angajament în avans). În plus, oferă instanțe spot, permițând clienților să cumpere mașini virtuale (VM) din excesul de capacitate a Azure cu reducere.

Utilizatorii pot porni sau opri serviciul după cum este necesar și pot plăti doar pentru secundele pe care le folosesc efectiv atunci când folosesc metoda cu plata pe măsură. Instanța rezervată, pe de altă parte, este concepută pentru utilizare continuă și se bazează pe costul pentru o lună întreagă (730 de ore), în timp ce modelul pay-as-you-go se bazează și pe analiza de 730 de ore, potrivit calculatorului de prețuri. Microsoft Azure permite o gamă largă de servicii, cum ar fi computere, rețele, stocare și analiză. Prin urmare, modelul său de prețuri depinde de diverși factori, inclusiv de capacitatea necesară, locația, tipul de serviciu și nivelul de management.

Prețuri Google. Este evident că Google a făcut un efort să învețe din greșelile rivalilor săi și a adoptat un model de cost pe secundă destul de simplu. În plus, GCP oferă un credit de 300 USD pentru un an de serviciu, o microinstanță gratuită pe lună pentru primul an al nivelului său gratuit și o reducere de 30% pentru utilizare continuă.

Oferă o serie de opțiuni de preț, cum ar fi prețuri cu plata măsurată după consum, rezervări pe termen lung și opțiuni gratuite. Costul Google Cloud este, de asemenea, influențat de o serie de factori, inclusiv prețul pentru calcul, SQL, rețele, stocare și serverless. Ar trebui să luați în considerare acești factori atunci când alegeți o structură de cost pentru orice afacere.

Google oferă clienților săi credit de 300 USD gratuit, deoarece clienții își pot cheltui suma pe produsele lor Google Cloud. Utilizatorii pot folosi, de asemenea, o varietate de produse gratuite, inclusiv cele mai populare servicii cloud disponibile în prezent pe piață pentru calcul, stocare, baze de date, IoT și inteligență artificială. În plus, gigantul tehnologic din SUA oferă reduceri semnificative pentru produsele care sunt „angajamentul de a utiliza" sau utilizate la un anumit nivel cu unul sau trei ani în avans.

Google oferă utilizatorilor săi o alegere specială cunoscută sub numele de „Sustained Use discounts (reduceri pentru utilizare susținută)". Dacă utilizați serviciile lunar într-un anumit procent, această ofertă va fi aplicată automat pe o scară variabilă. În plus, nu vi se cere să efectuați plăți în avans sau să semnați nici un angajament pentru a combina instanțe care nu se suprapun și pentru a primi beneficiile unei reduceri procentuale până la nivelul maxim.

Iată un grafic care arată comparațiile de prețuri între platforme (vezi Figura 2.8.):

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.

Figura 2.8. Comparația costurilor cloud între: AWS, Azure şi GCP

Întrebări de luat în considerare

- Care este cea mai atrăgătoare structură de preț pentru tine și de ce?
- De ce este dificil să faci o comparație directă a prețurilor între concurenți?
- Numiți cele două aspecte pe care toți cei 3 concurenți le împărtășesc și luați în considerare modul în care ați putea vinde platformele pe baza diferențelor dintre ele.

2.3 Selecting and setting the infrastructure

2.3.1 Implementarea Serverelor şi a Load Balancers-urilor (Echilibratorilor de Încărcare) pe toate Platformele Informatice

În această unitate, vom vedea rolul Load Balancer-ului (echilibrator de încărcare), care este o metodă de a ajuta o rețea să evite timpii morți supărători și să ofere utilizatorilor o performanță optimă prin procesarea sarcinilor și direcționarea sesiunilor pe diferite servere. Acest lucru se face în mod diferit în diferite rețele cloud. În această unitate, vom examina principalele 3 cazuri: AWS, Azure și Google Cloud Services.

Ce este un Load Balancer (echilibrator de încărcare)?
Un Load Balancer împarte traficul utilizatorilor între mai multe instanțe ale aplicațiilor dumneavoastră. Echilibrarea sarcinii reduce probabilitatea apariției unor probleme de performanță în aplicațiile dumneavoastră prin repartizarea sarcinii. Cloud Load Balancing (echilibrator de încărcare în cloud) este un serviciu gestionat definit prin software, complet distribuit. Deoarece nu se bazează pe hardware, nu vi se cere să gestionați o infrastructură fizică de echilibrare a sarcinii.

Load Balancers-urile (Echilibratoarele de încărcare) sunt clasificate în funcție de platforma lor, iar aici vom compara platformele cu unele dintre principalele Load Balancers-uri prin grafice care ilustrează cazurile:
Servicii Web Amazon (AWS)
Elastic Load Balancing (ELB)-(echilibarea elastică de încărcare) distribuie automat traficul de aplicații primite între mai multe obiective și dispozitive virtuale din una sau mai multe zone de disponibilitate (AZ-Availability Zones). O aplicaţie Load Balancer ia decizii de rutare la nivelul straturilor de aplicații (HTTP/HTTPS), sprijină rutarea bazată pe traseu și poate ruta solicitările către unul sau mai multe porturi pe fiecare instanță de container din clusterul dvs. Maparea dinamică a porturilor gazdă este suportată de aplicaţia Load Balancers. Iată o diagramă care prezintă aplicaţia Load Balancer pentru AWS (vezi Figura 2.9.):

Figura 2.9. Aplicația Load Balancer pentru AWS

Un echilibrator de încărcare de rețea (Network Load Balancer) ia decizii de rutare la nivelul de transport (TCP/SSL). Acesta poate procesa milioane de cereri pe secundă. Atunci când se primește o conexiune, echilibratorul de încărcare utilizează un algoritm de rutare hash flux pentru a selecta o țintă din grupul de ținte pentru regula implicită. Acesta încearcă să stabilească o conexiune TCP la ținta selectată pe portul specificat în configurația ascultătorului. Acesta trimite cererea cu antetele neschimbate. Atunci când Load balancer-ul primește o conexiune, utilizează un algoritm de rutare hash flux pentru a selecta o țintă din grupul de ținte pentru regula implicită. Solicitările sunt considerate ca provenind de la adresa IP privată a Load balancer-ului aparținând rețelei atunci când sunt configurate cu adrese IP ca ținte. Acest lucru înseamnă că, odată ce permiteți cererile primite și verificările de sănătate în grupul de securitate al țintei, serviciile din spatele unui Network Load Balancer sunt efectiv deschise lumii (dupa cum se vede in Figura 2.10.).

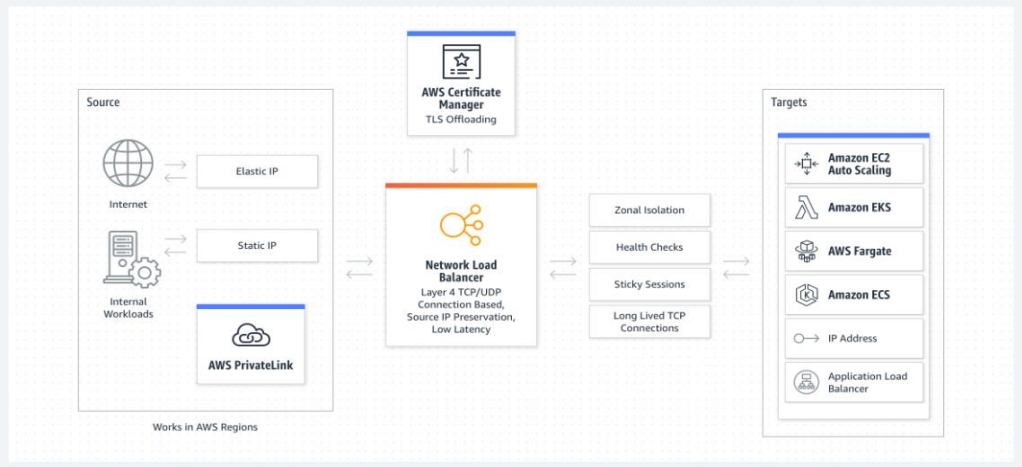

Figura 2.10. Load balancer pentru rețea

Azure

Un load balancer în Azure este utilizat pentru a distribui sarcinile de trafic către mașinile virtuale backend sau seturile de scale ale mașinilor virtuale. Puteți utiliza un load balancer în mod mai flexibil prin definirea propriilor reguli de echilibrare a încărcării. Procesul de distribuire uniformă a încărcării (traficul de rețea care intră) între un grup de resurse backend sau servere este denumit echilibrare a încărcării. Puteți utiliza load balancer-ul Azure pentru a distribui traficul către mașinile virtuale backend. Un load balancer Azure asigură faptul că aplicația dvs. este întotdeauna disponibilă. Load balancer-ul Azure este un serviciu autogestionat.

Conexiunile de ieșire pentru mașinile virtuale (VM) din cadrul rețelei virtuale pot fi furnizate de un distribuitor de sarcină public. Aceste conexiuni sunt posibile prin convertirea adreselor IP private în adrese IP publice. Load balancers-urile (echilibratoarele de încărcare) publice sunt utilizate pentru a furniza un trafic de internet echilibrat către mașinile dumneavoastră virtuale. Atunci când sunt necesare doar IP-uri private la frontend, se utilizează un load balancer intern (sau privat). Load balancers-urile ajută la echilibrarea traficului în cadrul unei rețele virtuale. Într-un scenariu hibrid, un frontend de echilibrare a sarcinii poate fi accesat prin intermediul unei rețele locale.

Load balancers-urile sunt prezentate mai jos în Figura 2.11.

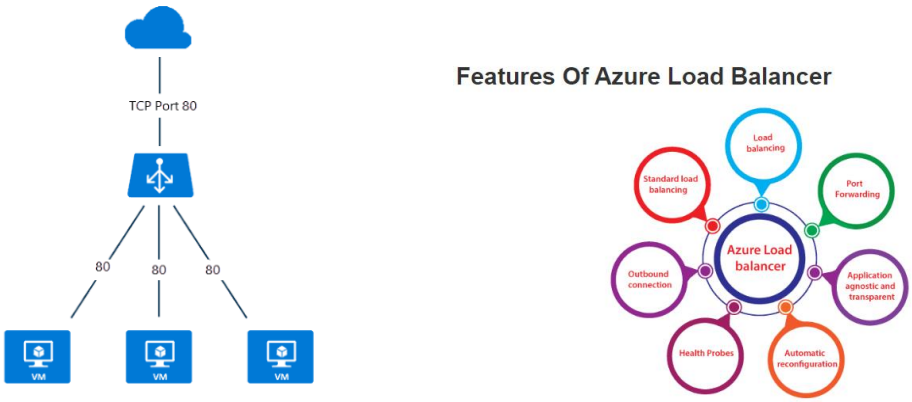

Figura 2.11. Load balancers

Unele dintre scenariile cheie pe care Azure le face prin intermediul unui Standard Load Balancer (echilibrator de încărcare standard) includ:

- Direcționarea traficului intern și extern către mașinile virtuale Azure.
- Distribuirea resurselor în interiorul și între zone pentru a crește disponibilitatea.
- Monitorizarea resurselor echilibratoarelor de sarcină cu sonde de sănătate.
- Prin intermediul Azure Monitor, se oferă măsurători multidimensionale.

GCS Cloud Load Balancing (echilibrator de încărcare pentru cloud GCS) este construit pe aceeași infrastructură care alimentează frontend-ul Google. Poate gestiona 1 milion sau mai multe interogări pe secundă, menținând în același timp o performanță ridicată și constantă și o latență scăzută. Traficul Cloud Load Balancing intră prin peste 80+ de locații globale distincte de echilibrare a încărcării, maximizând distanța parcursă pe coloana vertebrală rapidă a rețelei private Google. Puteți servi conținutul cât mai aproape de utilizatorii dvs. utilizând Cloud Load Balancing (Figura 2.12. de mai jos).

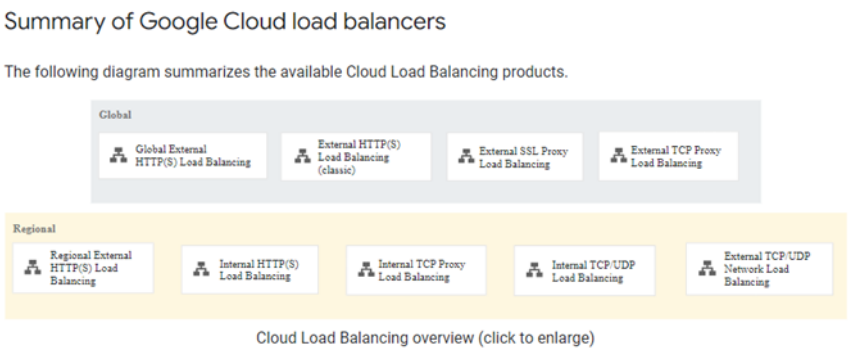

Figura 2.12. Alegerea unui Load Balancer (echilibrator de încărcare) pentru cloud

Pentru a alege un produs pentru echilibrarea încărcării în cloud, trebuie să stabiliți mai întâi ce tip de trafic trebuie să gestioneze load balancer-ul, precum și dacă aveți nevoie de echilibrare globală sau regională, echilibrare externă sau internă și echilibrare proxy sau prin trecere. Load balancer-ul din cloud poate echilibra traficul de încărcare către alte puncte finale diferite de cele din Google Cloud, cum ar fi centrele de date locale și alte cloud-uri publice accesibile prin conectivitate hibridă.

Diagrama din figura de mai jos (Figura 2.13.) ilustrează o implementare hibridă cu un distribuitor de sarcină HTTP(S) global extern.

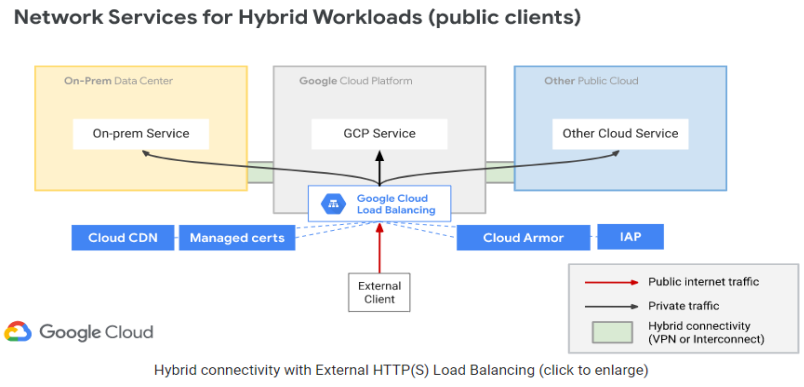

Figura 2.13. Implementare hibridă cu un load balancer HTTP(S) global extern

Un load balancer de rețea GCS poate accepta trafic de la

- orice client de internet.
- VM-uri Google Cloud cu IP-uri externe.
- Google Cloud VM care au acces la internet prin Cloud NAT sau NAT bazat pe instanță.

Caracteristicile echilibrării sarcinii rețelei în GCS sunt următoarele:

- Echilibrarea încărcării rețelei este un serviciu gestionat.
- Pentru a implementa echilibrarea încărcării rețelei sunt utilizate rețeaua virtuală Andromeda și Google Maglev.
- Load balancer-urile din rețele nu sunt proxy-uri.
- Mașinile virtuale de tip backend primesc pachete echilibrate în funcție de protocolul de încărcare cu adresele IP sursă și destinație, și, dacă protocolul este bazat pe port, porturile sursă și destinație neschimbate.
- Mașinile virtuale backend încheie conexiunile echilibrate în funcție de sarcină.

Mai jos (Figura 2.14.), puteți găsi un exemplu de Network Load Balancer (echilibrator de încărcare de rețea) în cazul unui utilizator:

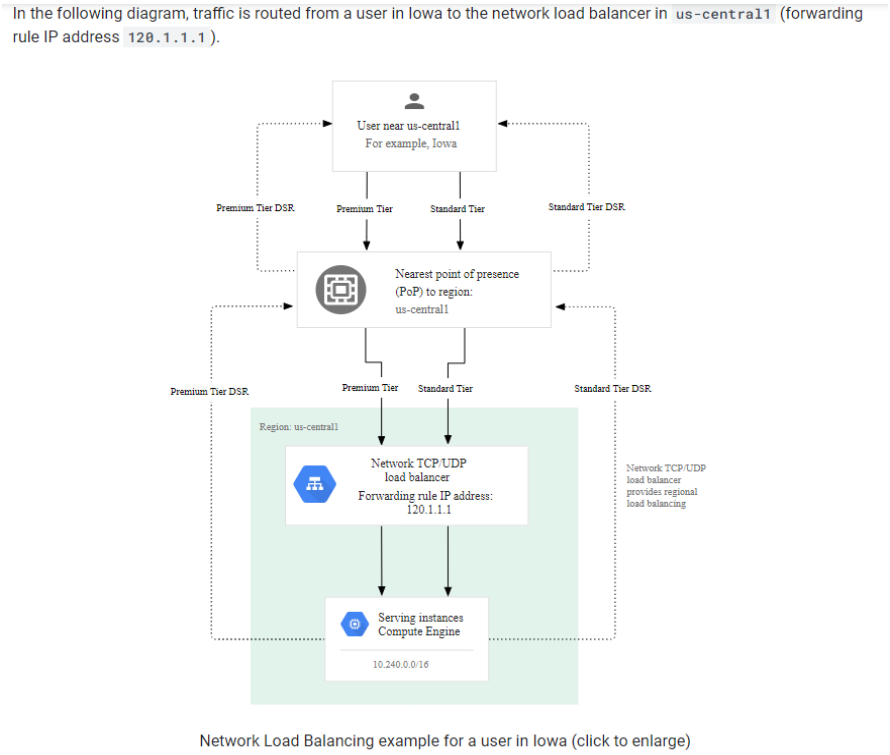

Figura 2.14. Network Load Balancer pentru un utilizator

Întrebări de luat în considerare:

1. De ce ar trebui să folosiți un Load balancer (echilibrator de încărcare)?

2. Numiți o caracteristică utilă din fiecare platformă cloud care trebuie luată în considerare .
3. Completați spațiile goale din această afirmație: Echilibrarea de încărcare din cloud este un serviciu administrat de _____,_____. Deoarece nu este _____, nu vi se cere să gestionați o infrastructură fizică de echilibrare a încărcăturii/ physical load balancing .
4. Numiți două dintre scenariile cheie pe care le face un Azure prin intermediul unui Standard Load Balancer (echilibrator de încărcare standard).

2.3.2 Servicii de stocare în cloud

Trei dintre cei mai mari furnizori de cloud Amazon Web Services (AWS), Google Cloud Platform (GCP) și Microsoft Azure (Azure) oferă trei tipuri principale de stocare pentru serviciile lor. Stocarea obiectelor, cunoscută și sub numele de stocare blob în Microsoft Azure, stocare bloc și stocare fișiere, toate având avantajele și dezavantajele lor și diferite cazuri de utilizare.

Pentru stocarea obiecte/blob, cele trei servicii principale sunt Serviciul de stocare simplu (S3) de la AWS, Stocarea în cloud de la Google și Azure Blobs de la Microsoft. Acestea trei fac toate în mare parte aceleași lucruri, cu unele variații în politicile și nivelurile de stocare pe care le oferă și punctele de preț pe care le au pentru stocarea pe GB și pentru accesarea fișierelor.

Toți cei trei furnizori au cel puțin trei niveluri de stocare generalizate, clasificate în ceea ce se numește stocare fierbinte (hot storage), stocare moderata(cool storage) si stocare la rece (cold storage). Aceste nume indică cât de des sunt accesate datele care sunt păstrate în stocare.

Stocarea fierbinte (hot storage) este pentru date care ar fi accesate frecvent și cu o latență cât mai mică posibil. Un exemplu de tip de date care ar trebui stocate în Hot storage ar fi imaginile produselor dintr-un magazin de comerț electronic. Clienții doresc să poată vedea fotografiile articolelor din magazin cu o latență cât mai mică, fără a fi nevoiți să aștepte ca site-ul să preia și să încarce imaginea în browserul lor.

Stocarea moderată (cool storage) este pentru date care ar trebui accesate rar. Un exemplu de stocare moderată ar fi un raport de vânzări cumulate. Datele din raport sunt accesate poate doar o dată pe lună pentru a se actualiza cu datele din luna precedentă, altfel accesul este minim. Este mult mai ieftin să stocați datele într-un nivel de stocare Cool decât în stocare Hot, dar vine în detrimentul unui preț mult mai mare pentru accesarea datelor și cu un timp minim de stocare.

O comparație a prețurilor între Stocarea caldă și Stocarea rece cu AWS S3:

Nivelul de stocare standard S3 cu un preț de aproape de două ori mai mult decât nivelul Acces infrecvent aşa cum se vede in Figura 2.15.

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

Figura 2.15. O comparație a prețurilor între Stocarea Hot și Stocarea Cool cu AWS S3

Accesul cu frecventă scăzută (S3 Infrequent Access) oferă un preț foarte mic pe GB.

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

Figura 2.16. Preţuri pentru accesul cu frecvenţă scăzută

Deci nivelul standard S3 oferă un preț mult mai mic pentru accesarea datelor stocate în bucket-uri.

	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

Figura 2.17. Preţuri standard pentru S3

Stocarea la rece este folosită pentru date care sunt accesate foarte rar, o dată sau de două ori pe an. Cel mai frecvent caz de utilizare este atunci când datele de arhivare care trebuie arhivate timp de câțiva ani din motive de reglementare, dar viteza de recuperare este un factor mai puțin important, având viteze de recuperare variind de la câteva minute până la 12 ore.

Unele date de arhivă care diferă ușor sunt anumite date de sănătate la care accesul este necesar foarte rar, dar atunci când este nevoie, trebuie să fie aproape instantaneu accesate.

Depozitarea la rece este cea mai ieftină dintre tipurile de depozitare când vine vorba de depozitare. Dar costul scăzut al stocării datelor vine cu un preț mult mai mare pentru accesul și regăsirea datelor.

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

Figura 2.18. Preţuri standard pentru S3

Figura 2.19. arată o comparaţie între preţurile la S3 Glacier Instant Retrieval, S3 Glacier Flexible Retrieval şi Deep Archive.

	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 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

Figura 2.19. Preţurile pentru S3 Glacier Instant, S3 Glacier Flexible si S3 Glacier Deep Archive

Stocare bloc: Amazon EBS, Azure Disks, Google Persisten Disk sau SSD local

Stocarea bloc este un tip de stocare în care volumele de stocare acționează ca unități de stocare, la fel ca unitățile de disc de pe un laptop fizic sau un computer desktop.

Datele sunt salvate pe aceste unități în blocuri de date de dimensiuni fixe. Acestor blocuri le se dau adrese unice, permițând software-ului de stocare bloc să găsească rapid locația datelor necesare. Aceste unități de stocare bloc pot fi, de asemenea, partajate între mai multe mașini virtuale diferite și sunt adesea folosite pentru stocarea datelor necesare aplicațiilor care sunt rulate în multe mașini virtuale diferite.

Unul dintre avantajele stocării bloc în comparație cu stocarea obiectelor este pentru datele în care fișierele mari trebuie schimbate și actualizate des. Cu o stocare bloc, trebuie doar să actualizați blocurile în care există date care sunt actualizate, în timp ce într-o stocare de obiecte ar trebui să actualizați întregul fișier de fiecare dată când se face o modificare.

Un alt caz de utilizare pentru stocarea în bloc este stocarea persistentă pentru aplicațiile care rulează pe mașini virtuale. Dacă o VM folosea doar stocarea locală alocată acelei VM, toate datele pe care le-ar scrie s-ar pierde ori de câte ori VM-ul ar trebui să repornească, deoarece nu veți avea niciodată nicio garanție că serverul care rulează o anumită instanță a unei VM ar fi la fel și data viitoare când se rulează instanța VM, astfel că toate datele scrise s-ar fi pierdut.

Stocare fișiere: Amazon EFS, Google Filestore, Azure Files

Atunci când alegeți clasa/nivelul de stocare, este important să luați în considerare nu numai prețul, ci și lucruri precum disponibilitatea serviciului, ce tip de tipare de acces vor fi utilizate (datele vor fi accesate de mai multe ori pe oră sau o dată pe lună, la cald la rece la foarte rece?) cât timp trebuie stocate datele?

De exemplu, AWS are S3 Intelligent Tier care monitorizează tiparele de acces la datele dvs. și trece între standardul S3 și nivelurile S3 Infrequent Access pentru a ajuta la scăderea costurilor de stocare, ceea ce este o soluție excelentă dacă modelul de acces sau datele dvs. nu sunt complet. cunoscut.

O altă considerație ar fi care furnizor este utilizat în restul întreprinderii și familiaritatea colegilor din ecosistemul furnizorului.

Diferiți furnizori au, de asemenea, centre de date în diferite părți ale lumii, așa că ar trebui luate în considerare care regiuni sunt disponibile şi cu ce servicii. Dacă stocarea dvs. este implementată în regiuni cât mai apropiate de utilizatorii dvs., va reduce latența de accesare a fișierelor stocate.

Acestea sunt toate considerentele care trebuie luate atunci când alegeți tipul de stocare și nivelul de stocare care este cel mai potrivit pentru datele pe care le aveți și care furnizor oferă cea mai bună soluție generală pentru nevoile dvs. specifice de afaceri.

În prezent, Amazon oferă 27 de regiuni diferite, Microsoft Azure având cele mai multe regiuni, cu 42. Google urmează cu 34 de regiuni.

Cum să creați un bucket folosind Consola Amazon AWS:

Când vă aflați în pagina de pornire a consolei, faceți clic pe pictograma din stânga sus care înseamnă „Services (Servicii)”. Aceasta va crea un meniu derulant cu o listă de servicii AWS. Derulați în jos și faceți clic pe „Storage (Stocare)”.

Aceasta va deschide un panou lateral care listează diferite servicii de stocare oferite de AWS. Faceți clic pe „S3”. Aceasta vă va duce la consola Amazon S3.

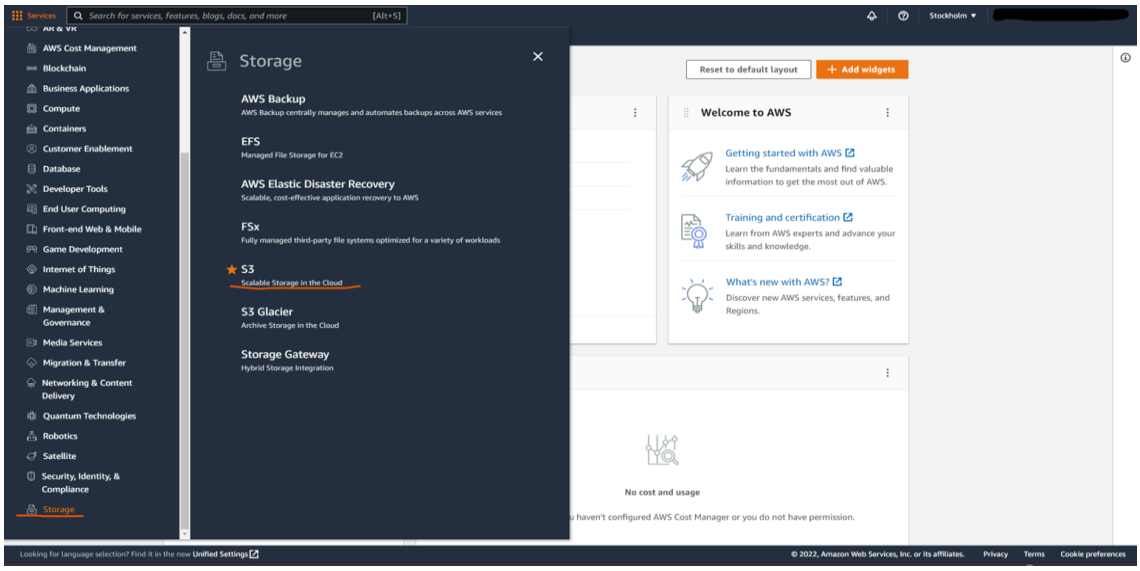

Figura 2.20. Consola S3

Când vă aflați în consola S3, veți primi o listă cu toate bucket-urile S3 din contul dvs.(după cum se arată în Figura 2.20.)

Dacă este prima dată când deschideți consola S3, nu vor fi bucket-uri.

Faceți clic pe butonul portocaliu din dreapta care spune „Create bucket (Creați un bucket)”(după cum se arată în Figura 2.21.).

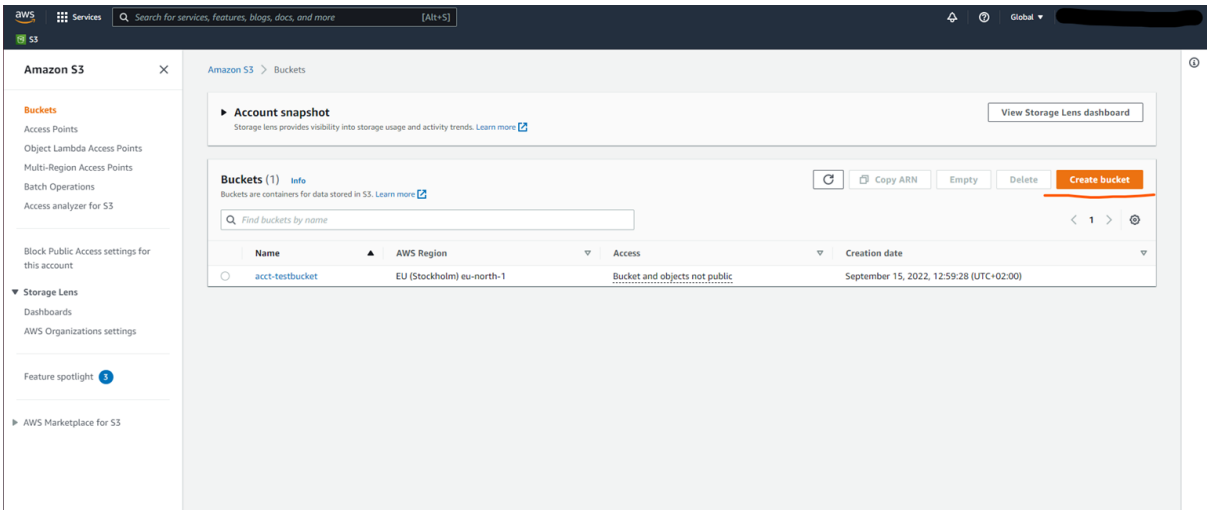

Figura 2.21. Creați un bucket în consola S3

După ce ați făcut clic pe butonul, vi se va afișa „Create bucket wizard (expertul de creare a unui compartiment)”.

Aici veți seta configurația pentru un bucket (vezi Figura 2.22.). Acestea includ numele unic la nivel global pentru bucket. Și regiunea AWS va fi stocată.

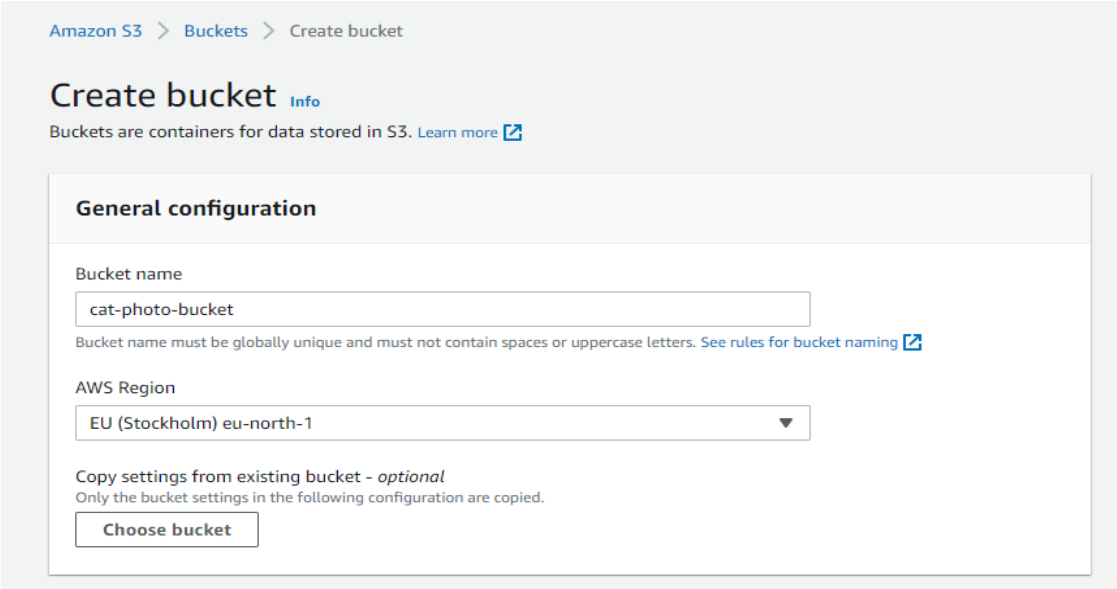

Figura 2.22. Setarea unui bucket în consola S3

Setarea regiunii corecte este importantă, deoarece setarea unui bucket într-o regiune care este departe de baza dvs. de utilizatori poate introduce latență în accesarea fișierelor stocate în bucket.

Apoi setați dreptul de proprietate asupra obiectelor care sunt stocate în bucket. Vom alege setarea recomandată lăsând Lista de control al accesului (ACL-Access control list) dezactivată. Aceasta înseamnă că proprietatea asupra obiectelor stocate va rămâne pentru contul căruia îi aparține bucket-ul

A doua setare din această imagine este Accesul Public (Public Access). Această setare vă permite să decideți dacă obiectele din bucket sunt sau nu accesibile din alte conturi pe baza diferitelor criterii descrise în expert.

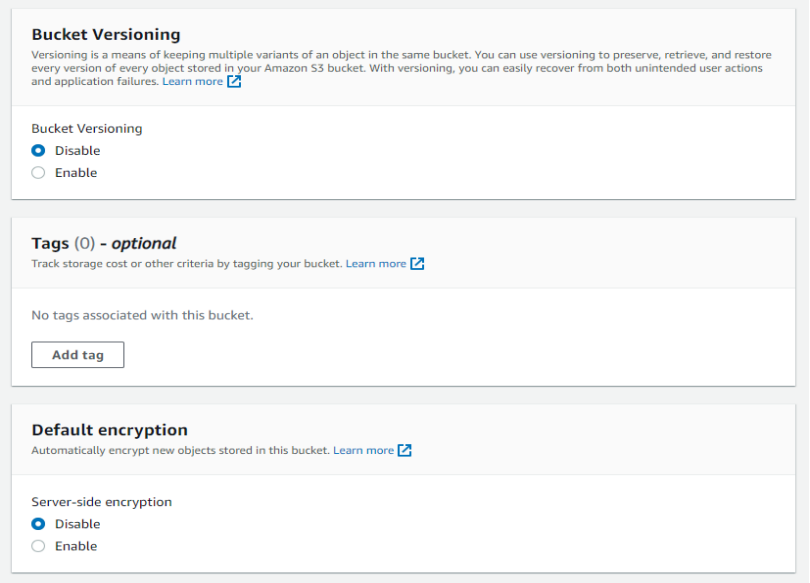

Figura 2.23. Activarea versiunii bucket-ului în consola S3

Versiunea bucket-ului (vezi Figura 2.23.) este folosită pentru a păstra o arhivă a tuturor iterațiilor diferite ale obiectelor din acesta. Utilizarea versiunilor vă permite să păstrați un jurnal al modificărilor și editărilor aduse grupului și, de asemenea, vă permite să rerulați sau să regăsiţ obiecte în cazul unei erori, cum ar fi o ștergere neintenționată.

Etichetele pot fi folosite pentru a oferi bucket-urilor dvs. o modalitate ușoară de a le grupa împreună, astfel încât acestea să poată fi utilizate, de ex. alocarea costurilor, asigurând faptul că costurile asociate unui anumit proiect sunt urmărite corespunzător.

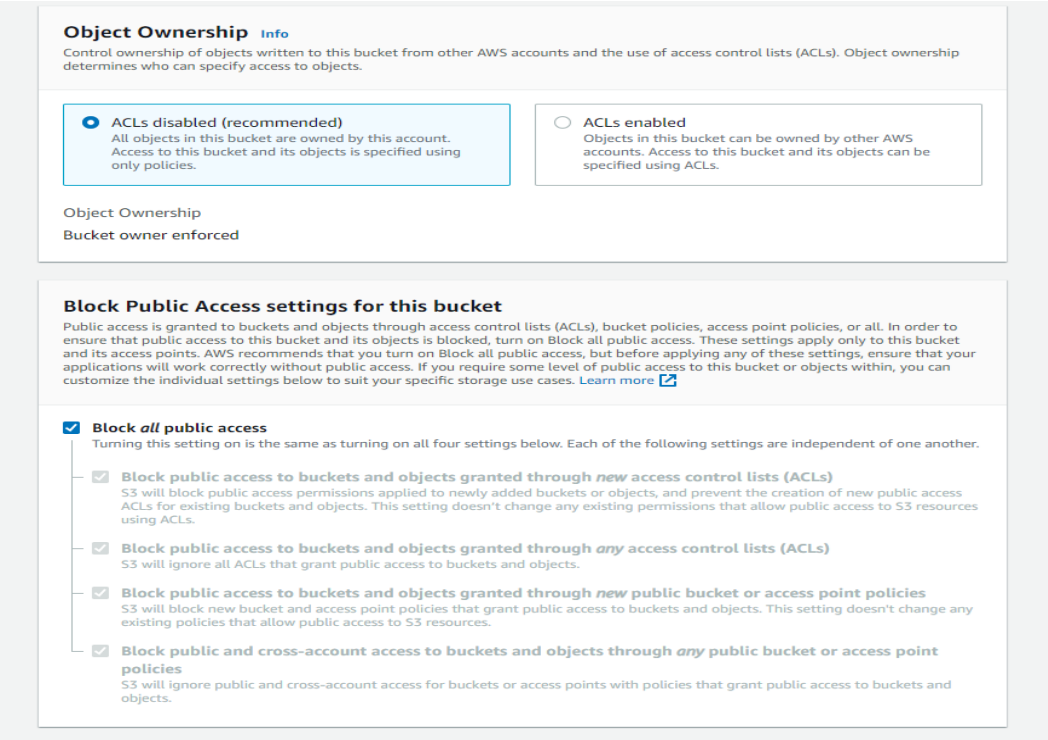

Figura 2.24. Proprietatea obiectului în consola S3

Criptarea implicită vă permite să decideți dacă doriți ca obiectele din compartiment să fie criptate înainte ca AWS să le salveze în bucket, lăsându-le criptate în timpul repausului și să le decripteze numai când sunt descărcate din nou. Activarea criptării necesită să configurați o cheie pentru criptarea și decriptarea obiectelor folosind fie chei gestionate de Amazon S3 (SSE-S3), fie AWS Key Management Service.

Sub setările avansate putem prescrie ca în bucket să aibă loc o blocare a obiectelor (vezi Figura 2.25.). Activarea blocării obiectelor înseamnă că obiectele stocate nu pot fi șterse sau modificate în timp ce blocarea este în vigoare. Acesta se numește model Write-Once-Read-Many (scrie odată citeşte de mai multe ori) sau model WORM.

După ce s-a terminat toată configurația, faceți clic pe butonul „Create bucket (Creare bucket)”.

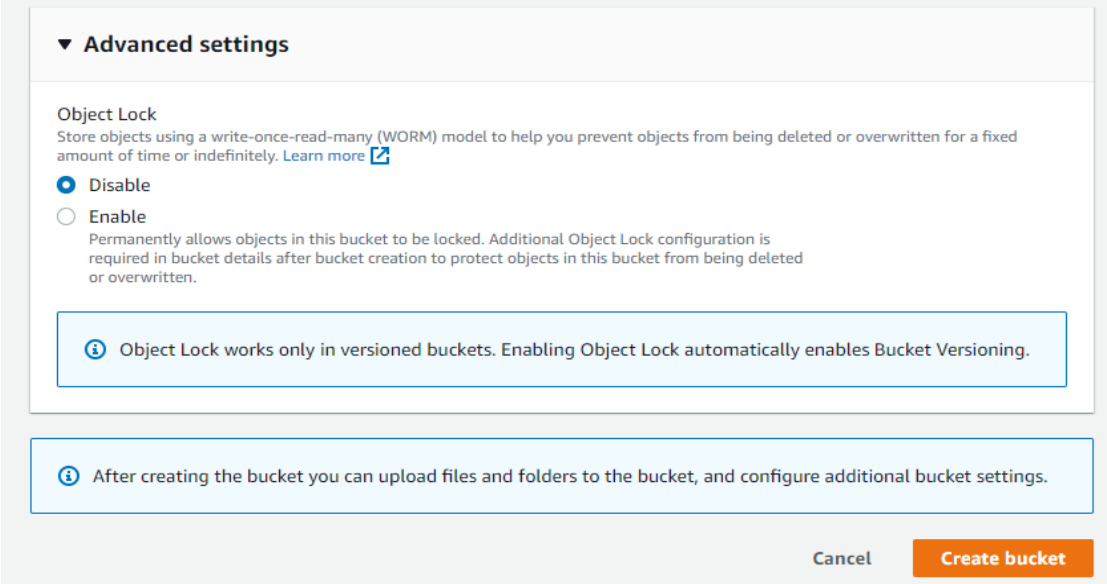

Figura 2.25. Finalizarea configurării în consola S3

După ce ați creat bucket-ul, veți fi dus înapoi la pagina consolei S3 și noul dvs. bucket va fi listat în tabelul cu bucket-uri și este acum gata pentru a vă stoca fișierele.

Pentru a începe să încărcați fișiere în acest bucket nou creat, faceți clic pe nume. Astfel se va deschide compartimentul (vezi Figura 2.26.).

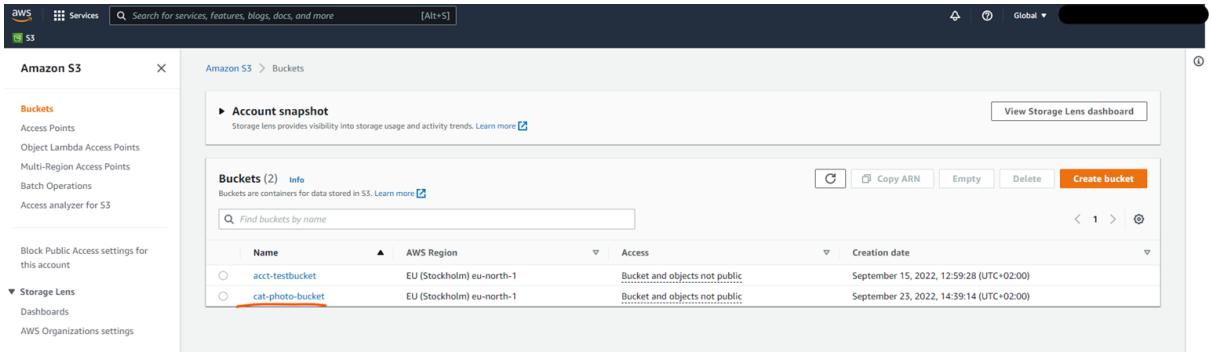

Figura 2.26. Încărcarea fișierelor în bucket-ul nou creat în consola S3 - primul pas

Aici puteți vedea o mulțime de informații despre bucket, cum ar fi obiectele stocate, iar în fila de proprietăți puteți vedea și edita o parte din configurația care a fost setată în timpul creării.

Pentru a încărca un fișier în bucket, puteți face clic pe oricare dintre cele două butoane Upload (Încărcare) sau puteți glisa și plasa fișierele din exploratorul de fișiere (vezi Figura 2.27.).

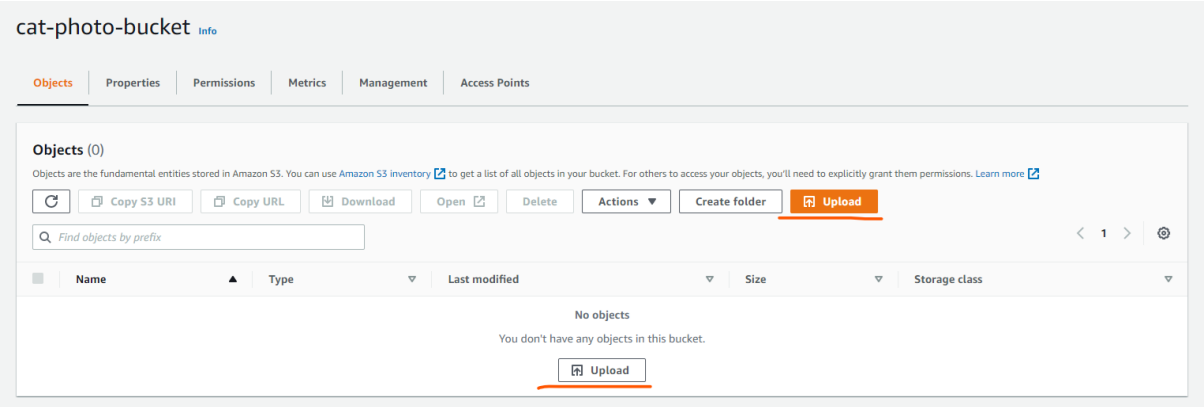

Figura 2.27. Încărcarea fișierelor în bucket-ul nou creat în consola S3 – pasul doi

Făcând clic pe unul dintre butoanele „Upload (Încărcare)” vă duce la următorul ecran, aici vi se oferă posibilitatea de a alege între a încărca fișiere individuale sau a încărca un folder întreg. Puteți fie să faceți clic pe butoanele „Add (Adăugați)”, acest lucru va deschide un nou explorator de fișiere, și puteți alege fișierele sau folderele pe care doriți să le încărcați, în funcție de care dintre cele două butoane au fost acţionate.

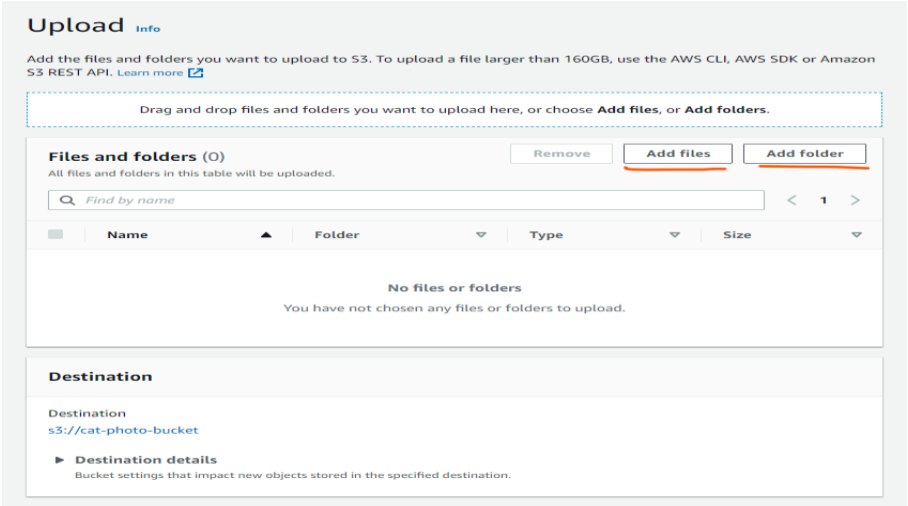

Figura 2.28. Încărcarea fișierelor în bucket-ul nou creat în consola S3 – pasul trei

În exemplul nostru, am încărcat trei imagini. Rețineți că destinația este bucket-ul creat de noi (vezi Figura 2.28.). Deschiderea detaliilor despre destinație va afișa unele dintre setările grupului care au fost specificate. Versiune (Versioning), Criptare Implicită (Default Encryption) și Blocare Obiect (Object Locking).

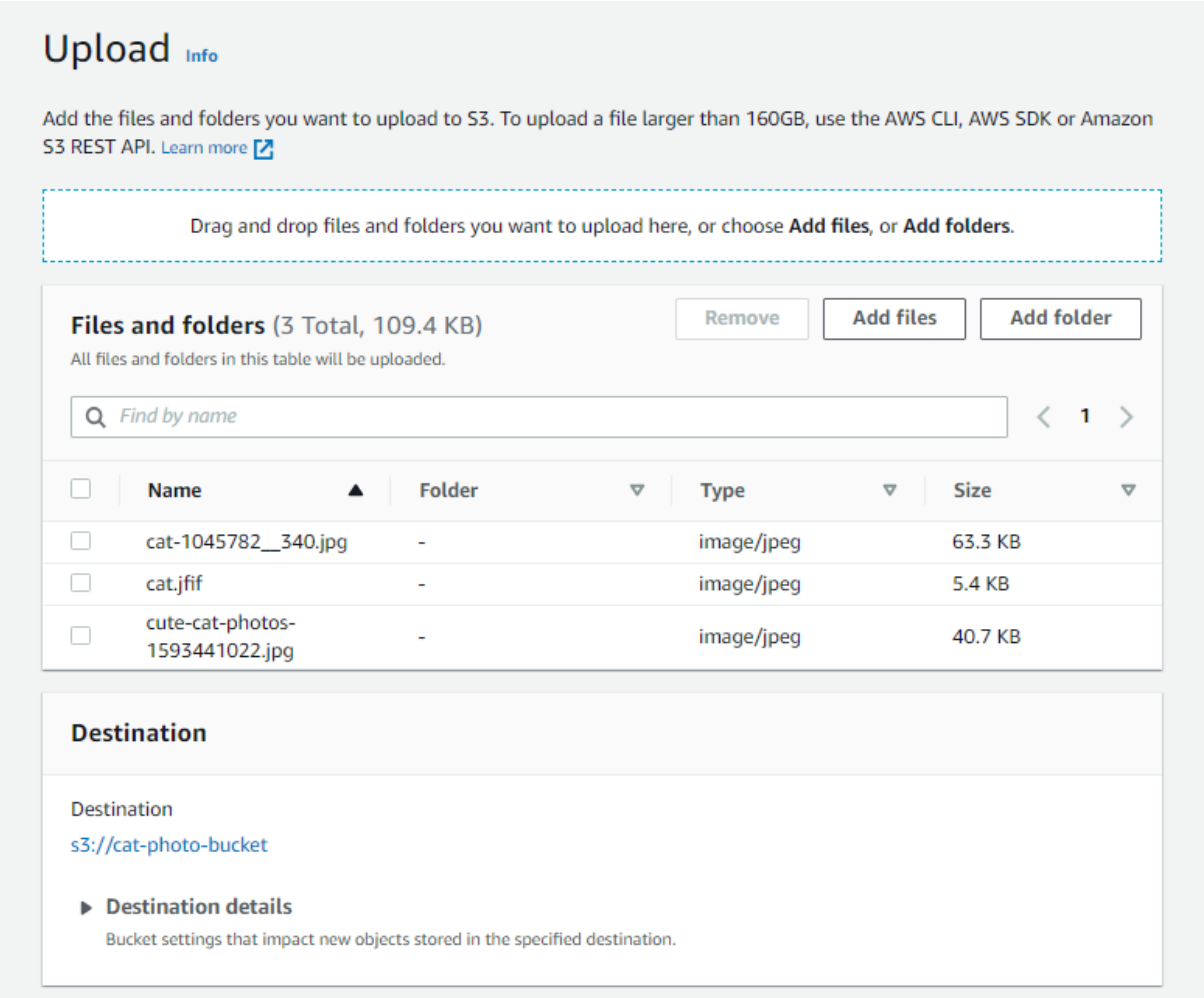

Figura 2.29. Încărcarea imaginilor în grupul nou creat din consola S3

Apoi avem proprietățile (vezi Figura 2.30.). Aici puteți seta ce clasă de stocare doriți să utilizați pentru fișierele sau folderele care sunt încărcate.

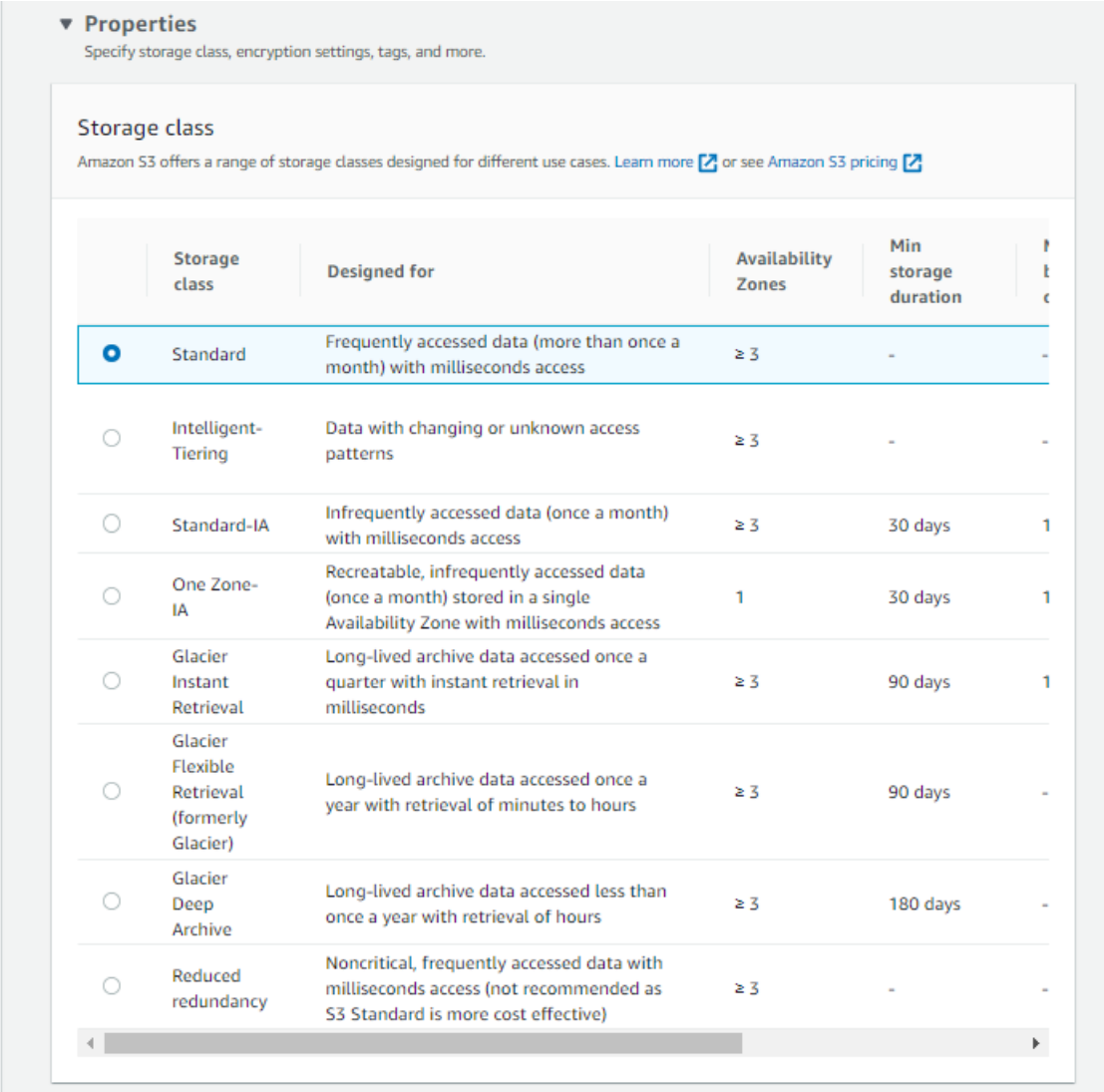

Figura 2.30. Proprietatea obiectului din consola S3

De asemenea, puteți activa sume de control suplimentare, aceasta vă permite să setați propria funcție sumă de control pentru a vă asigura că integritatea obiectelor este validă.

Etichetele sunt similare cu cele menționate mai devreme în timpul creării compartimentului, iar metadatele sunt date care descriu într-un fel datele în sine, cum ar fi tipul de conținut sau numele de utilizator al persoanei care creează fișierul original.

Când toate acestea sunt setate, faceți clic pe butonul Upload (Încărcare) și fișierele dvs. vor fi stocate în cloud!(vezi Figura 2.31.)

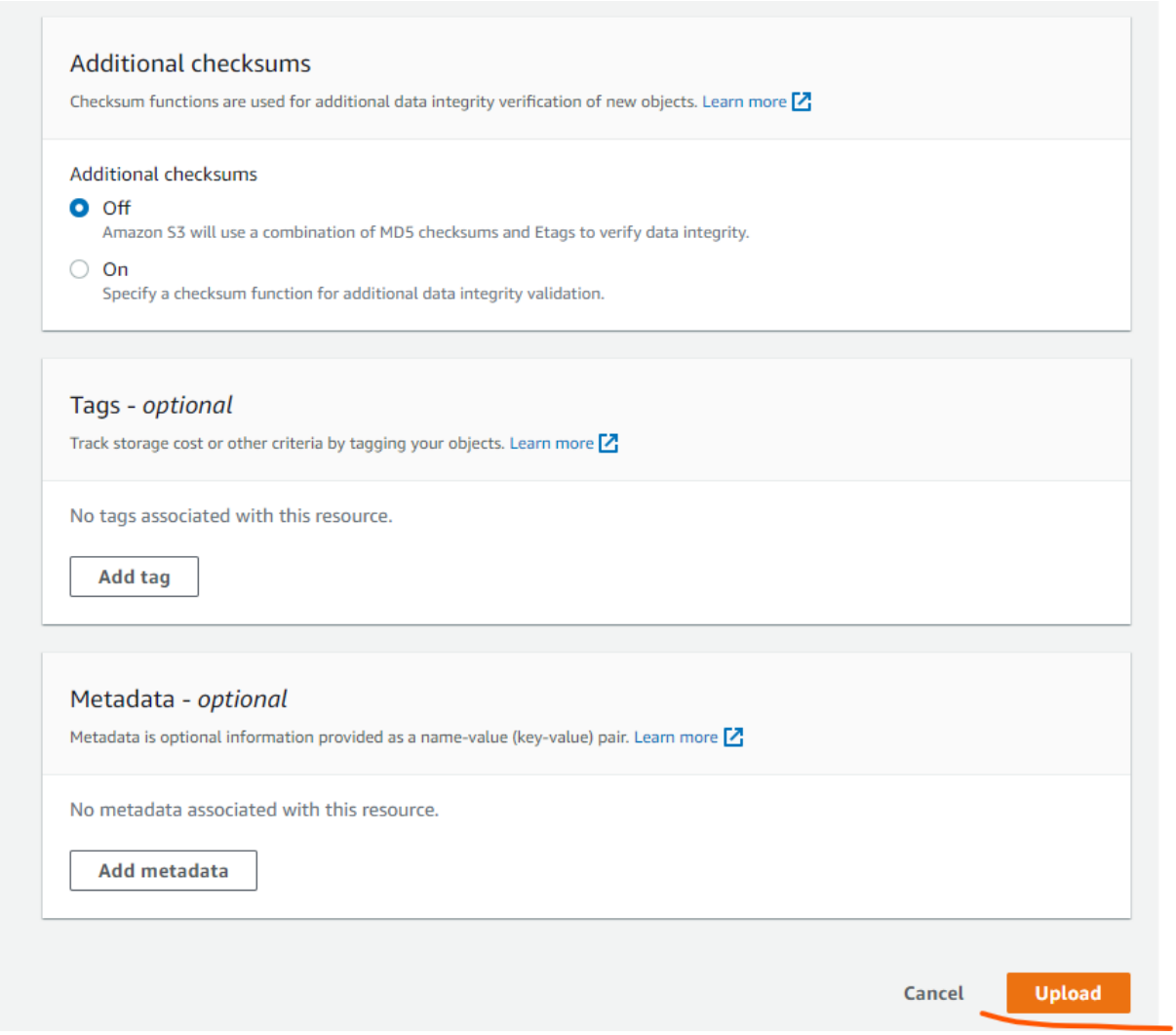

Figura 2.31. Încărcare în consola S3

După ce încărcarea este finalizată, o să vedem că avem un mesaj de succes în partea de sus și putem vedea lista celor trei imagini ale noastre în tabelul de fișiere și foldere cu câteva date suplimentare despre tipul și dimensiunea fișierelor și mesajul de stare.

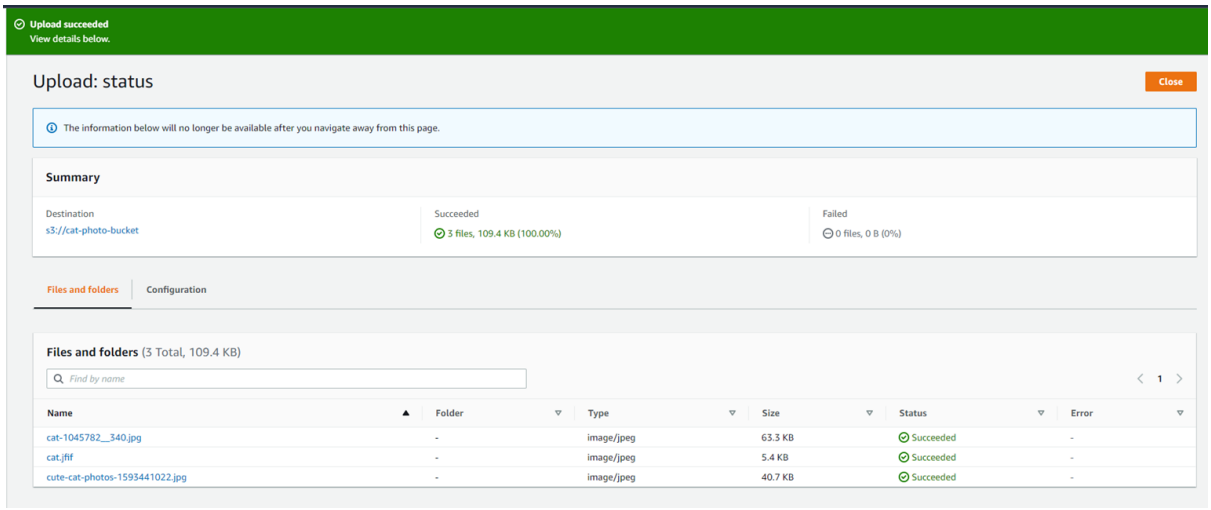

Figura 2.32. Consola S3 – mesajul care exprimă încărcarea cu succes

Făcând clic pe butonul de Închidere (Close), suntem duși înapoi la bucket și acum putem vedea că avem trei fișiere în tabelul nostru de obiecte și câteva informații despre fișiere, cum ar fi tipul, dimensiunea și clasa de stocare folosită pentru a le stoca. (vezi Figura 2.33.).

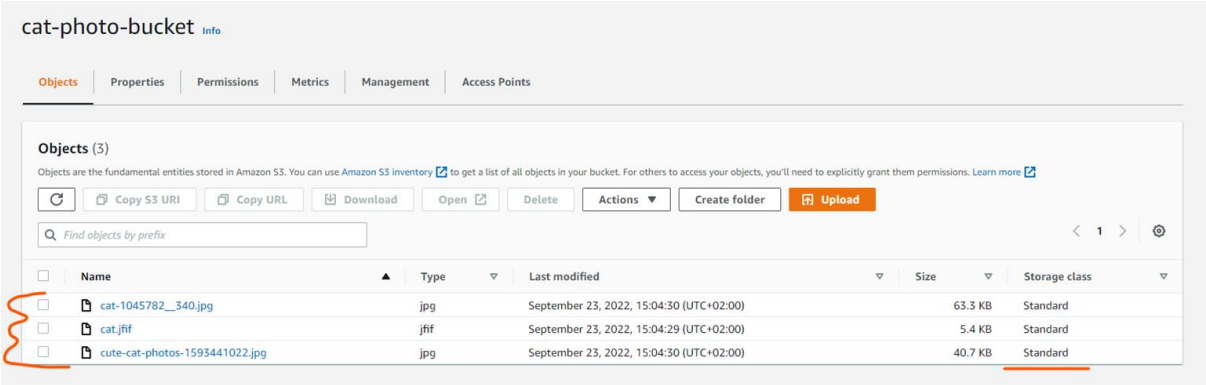

Figura 2.33. Informaţii despre datele stocate în consola S3

Acum că avem fișierele noastre în cloud, putem prelua aceste fișiere din cloud. Bifați caseta de selectare de lângă numele fișierului pe care doriți să-l preluați și veți observa că butoanele gri de pe rândul de deasupra tabelului sunt acum disponibile. Faceți clic pe butonul Descărcare (Download) și veți începe descărcarea fișierului pe computer. Adresa URL copiabilă și URI-ul S3 pot fi, de asemenea, folosite pentru a accesa obiectele, dar în cazul nostru lipirea URL-ului în browser vă va oferi doar un mesaj de eroare care spune că nu avem acces.

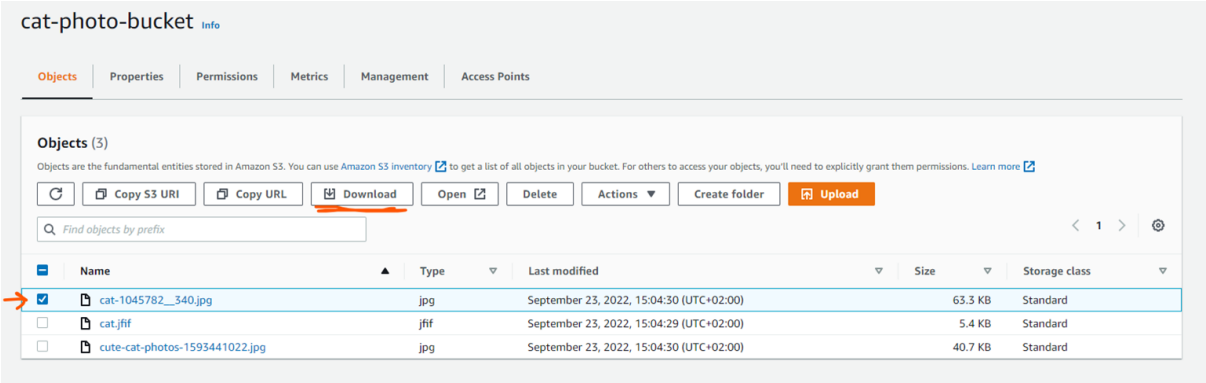

Figura 2.34. Consola S3 – recuperarea fişierelor din cloud

Uneori trebuie să ștergeți obiecte dintr-un bucket (vezi Figura 2.35.). Trebuie doar să selectați fișierele sau folderele pe care doriți să le ștergeți, bifând caseta Name (Nume) de lângă fişiere, selectând astfel toate obiectele din bucket sau selectați fiecare fișier individual, așa cum am făcut când am preluat fișierul.

După ce toate obiectele pe care doriți să le ștergeți au fost selectate, faceți clic pe butonul de ștergere.

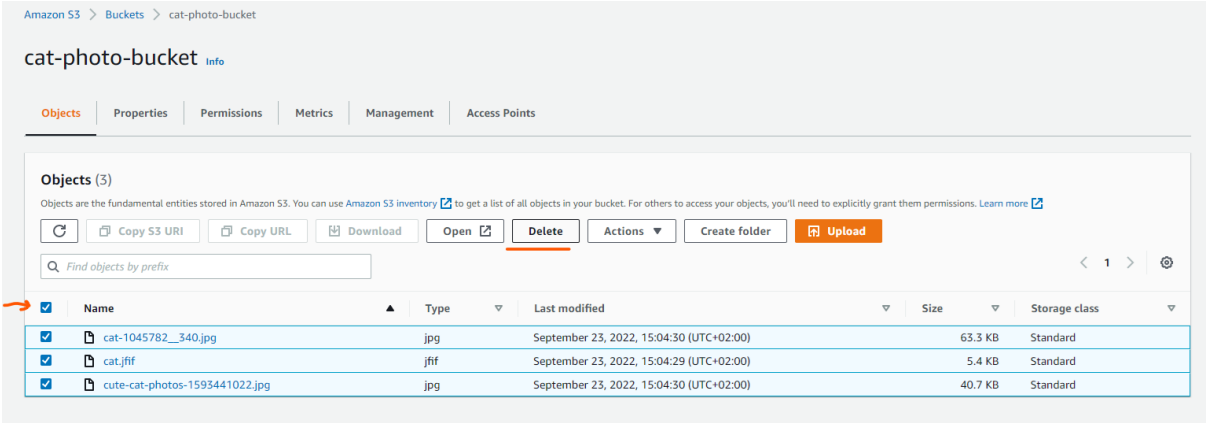

Figura 2.35. Consola S3 - ştergerea obiectelor dintr-un bucket

După ce faceți clic pe butonul de ștergere, vi se va cere să confirmați ștergerea cu un avertisment despre consecințele acțiunii. Confirmați ștergerea introducând textul solicitat „permanently delete' (ștergeți definitiv)" în câmpul de text și faceți clic pe buton pentru a continua. După ce ați făcut clic pe buton, veți fi redirecționat către un rezumat al acțiunii care arată dacă a avut succes sau dacă au apărut erori.

Faceți clic pe Close (Închidere) și veți fi redirecţionat înapoi la pagina unde toate obiectele din bucket au dispărut acum.

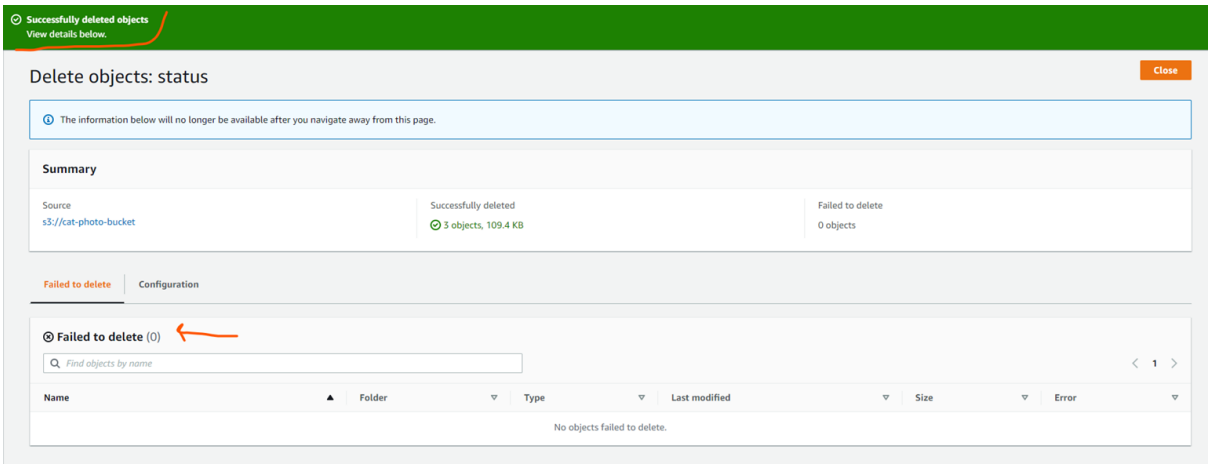

Figura 2.36. Consola S3 –starea obiectului șters

Acum că este gol, putem elimina în siguranță compartimentul din cont. Pentru a șterge compartimentul în sine, trebuie doar să selectați bucket-ul pe care doriți să îl ștergeți bifând butonul radio pentru categoria corectă și faceți clic pe butonul de ștergere de lângă butonul de creare a bucket-ului pe care l-am folosit mai devreme (vezi Figura 2.37)

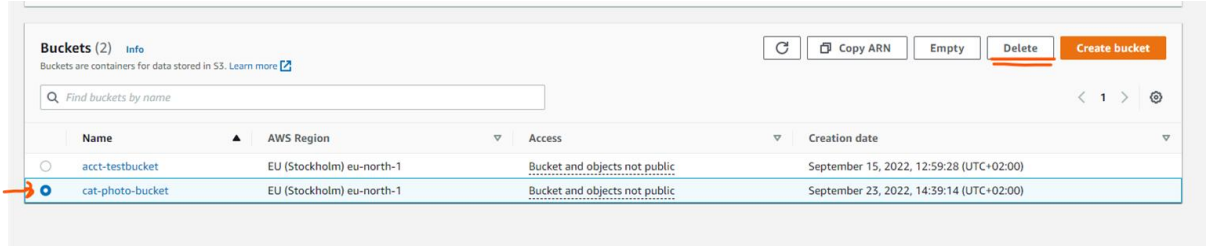

Figura 2.37. Consola S3 – ştergerea bucket-ului

La fel ca atunci când am șters obiectele din bucket, vi se va solicita să confirmați ștergerea introducând numele bucket-ului și făcând clic pe butonul Delete bucket (Ștergere bucket). După ce ștergerea s-a încheiat, veți fi redirecționat către pagina principală S3, unde bucket-ul dvs. nu va mai fi listat în tabelul de compartimente.

2.3.3 Managementul accesului de identitate

Managementul de identitate (IAM- Identity Access Management) este o modalitate de a gestiona atât autentificarea unui reprezentant legal, fie că este un utilizator uman sau o mașină care accesează printr-un API, cât și autorizarea aceluiași reprezentant și permite accesul membrilor unui cont sau organizație către infrastructura cloud pe baza permisiunilor care sunt acordate de către serviciul IAM.

Serviciul IAM poate stabili politici la mai multe nivele, cum ar fi utilizatorii individuali sau pentru grupuri. Deci ce este autentificarea şi autorizarea şi care este diferenţa?

Autentificarea este actul de validare a oricăruia care încearcă să acceseze resursele dvs. cloud, şi este cine pretinde că este. Acest lucru se poate face folosind:

- Nume de utilizator și parolă
  - Cel mai comun mod de a autentifica utilizatorii. Acest mod cere oricui care încearcă să se autentifice să furnizeze o combinație de nume de utilizator și parolă care este apoi verificată de un sistem și, dacă se potrivește cu ceea ce este înregistrat în acel sistem, rezultă că utilizatorul verificat este cine pretinde a fi.
- Pin pentru o singură utilizare (One-time pins)
  - Aceasta este o modalitate de validare în care utilizatorul solicită acces la sistem printr-un PIN generat automat, care de obicei durează doar pe durata sesiunii utilizatorului sau pentru o singură tranzacție.
- Aplicații de autentificare
  - Un sistem terț de încredere generează o parolă pe care să o utilizeze un utilizator.
- Biometrie
  - Biometria cere utilizatorului să-și verifice identitatea printr-o amprentă digitală, scanarea ochilor sau recunoașterea feței

Din ce în ce mai mult vedem că se utilizează autentificarea multifactorială (MFA). Acest lucru necesită ca oricine încearcă să se autentifice trebuie să se verifice cu succes prin două sau mai multe dintre metodele menționate mai sus. Aceste metode sunt adesea plasate în trei categorii principale; Ceva ce știi, ceva ce ai și ceva ce ești.

Acestea vor fi foarte adesea parola dvs., o aplicație pentru telefon și, respectiv, o parte biometrică. După ce utilizatorul a fost verificat cu succes, acesta trebuie, de asemenea, să fie autorizat înainte de a putea începe să acceseze resursele din sistemul cloud.

Autorizarea este, în acest context, un proces în care sistemul verifică dacă utilizatorul, care a fost autentificat anterior, are permisiunile necesare pentru a efectua acțiunea pe care încearcă să o facă. Un exemplu în acest sens ar putea fi un depozit de imagini în care utilizatorii obișnuiți au voie să vizualizeze și să descarce imaginile de pe site, dar numai utilizatorii cu privilegii de administrator au voie să încarce imagini în depozit (vezi Figura 2.38).

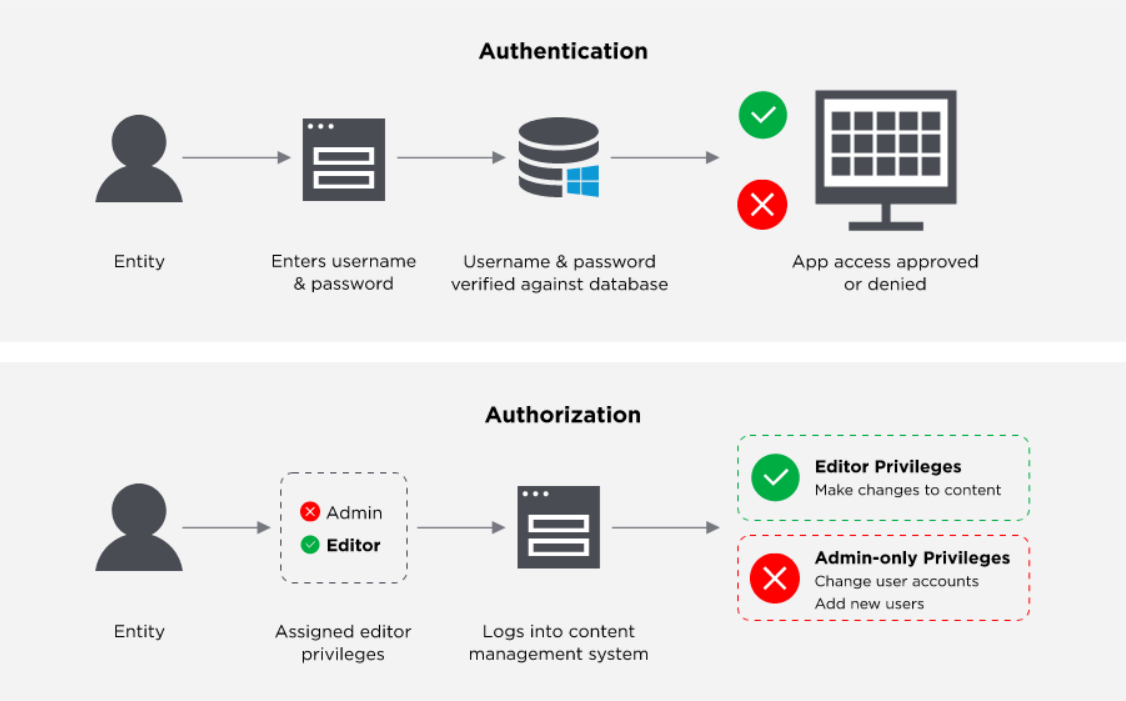

Figura 2.38. Autorizarea

Toți cei trei mari furnizori de servicii cloud oferă un serviciu de gestionare a identității și a accesului. Microsoft Azure îl numește Azure Active Directory. Amazon l-a numit AWS IAM și în Google Cloud se numește doar IAM.

Managementul identității și accesului vă ajută să controlați în siguranță accesul la serviciile Cloud pe care le utilizați, cum ar fi un bucket AWS S3 sau o instanță Microsoft Azure CosmoDB. Vi se permite să creați mai mulți utilizatori IAM sub umbrela contului dvs. principal, care manevrează toate resursele.

Pentru a gestiona accesul la resursele dvs. cloud, fără să utilizați, de exemplu, AWS IAM, ar fi trebuit să creați mai multe conturi AWS, fiecare dintre acestea să aibă propria facturare și abonamente separate la diferitele produse AWS. Sau toți angajații din organizația dvs. care trebuie să utilizeze AWS ar trebui să partajeze acreditările pentru un singur cont AWS, fără a exista nici o modalitate de a restricționa accesul angajaților la resurse pe care nu au nevoie să le acceseze.

Cu IAM, totuși, este posibil să configurați mai mulți utilizatori într-un singur cont AWS, începând cu utilizatorul la nivel rădăcină pe care AWS îl creează automat la crearea contului. Fiecare utilizator ulterior adăugat la cont va avea propriile acreditări. Acești utilizatori, fie ei umani sau mașini, pot avea, de asemenea, acces la resurse specifice din AWS prin utilizarea politicilor care în AWS sunt definite în format JSON (vezi Figura 2.39.).

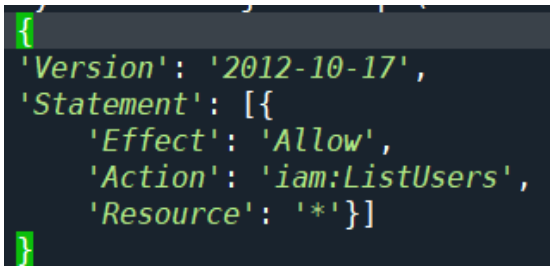

Figura 2.39. Acordarea accesului la resurse din AWS

Aceste politici sunt atașate utilizatorilor fie direct, fie printr-un grup de utilizatori.

Un grup de utilizatori este o resursă IAM pe care o puteți folosi pentru a adăuga mai mulți utilizatori IAM, astfel încât să puteți atașa cu ușurință mai multe politici oricărui utilizator prin adăugarea acestuia la un grup de utilizatori. De exemplu, dacă aveți un rol în cadrul organizației dvs. care necesită ca utilizatorii să poată crea și șterge bucket-uri S3, ori de câte ori o persoană nouă primește acest rol, administratorul IAM poate pur și simplu să adauge contul de utilizator IAM al utilizatorului respectiv la grupul de utilizatori, mai degrabă. decât să atașeze manual toate politicile necesare utilizatorului.

Toate trei oferă aceeași funcționalitate de bază pentru autentificarea utilizatorilor asociați cu contul sau organizația lor și pentru autorizarea acestor utilizatori ca să acceseze resursele de care au nevoie prin politici de acces care sunt atașate utilizatorilor într-un fel.

Resurse IAM

Obiectele utilizator, grup, rol, politică și furnizor de identitate care sunt stocate în IAM. Ca și în cazul altor servicii AWS, puteți adăuga, edita și elimina resurse din IAM.

Identități IAM

Obiectele resursă IAM care sunt utilizate pentru a identifica și grupa. Puteți atașa o politică la o identitate IAM. Acestea includ utilizatori, grupuri și roluri.

Entități IAM

Obiectele de resurse IAM pe care AWS le folosește pentru autentificare. Acestea includ utilizatorii și rolurile IAM.

Reprezentanți legali

O persoană sau o aplicație care utilizează user-ul root al contului AWS, un utilizator IAM sau un rol IAM pentru a se conecta și a face solicitări către AWS. Reprezentanții legali includ utilizatori federalizați și roluri asumate.

Modele și principii

Principiul celui mai mic privilegiu:

Principiul celui mai mic privilegiu, sau Just-Enough-Access, este una dintre pietrele de temelie ale managementului accesului și prevede ca unui utilizator sau aplicație ar trebui să i se acorde doar cel mai mic acces necesar pentru a îndeplini sarcina pe care o face. De exemplu, dacă o aplicație este utilizată pentru a afișa imagini care sunt stocate într-o înmagazinare de obiecte, adică stocarea blob Azure, acea aplicație va trebui să citească doar din acel spațiu de stocare, ca atare nu ar trebui să i se acorde nimic în afară de accesul pentru citire.

Model cu încredere zero:

Modelul cu încredere zero (zero-trust model) este un model de securitate în care se presupune că integritatea rețelei a fost compromisă și că nu există puncte de acces în mod inerent sigure.

Acest lucru este contrar vechilor modele tradiționale de securitate în care o rețea a fost închisă de restul internetului și doar computerele de încredere și gestionate ar fi permis să se alăture. Rețeaua ar acorda apoi acces la aceste computere și dispozitive în funcție de locația lor și de faptul că li s-a dat acces la rețea.

Cu modelul Zero-trust (Încredere zero), toate dispozitivele sunt tratate ca și cum ar veni dintr-o locație nesigură și solicită autentificarea tuturor pentru a-și dovedi identitatea înainte de a obține acces la activele și resursele de care au nevoie.

Doar pentru un timp (just in time):

Accesul just in time este un model de securitate în care un firewall va restricționa orice și tot traficul de intrare la o resursă până când un utilizator solicită acces. Utilizatorul va trebui să-și, verifice autorizarea iar dacă cererea este aprobată, regulile pentru traficul de intrare la resursa solicitată sunt modificate temporar pentru a permite accesul utilizatorului respectiv și apoi le va schimba înapoi pentru a interzice orice alt trafic.

RBAC & ABAC

Controlul accesului bazat pe roluri (RBAC) și Controlul accesului bazat pe atribute (ABAC) sunt două dintre cele mai comune metode de securizare a accesului la resursele din cloud.

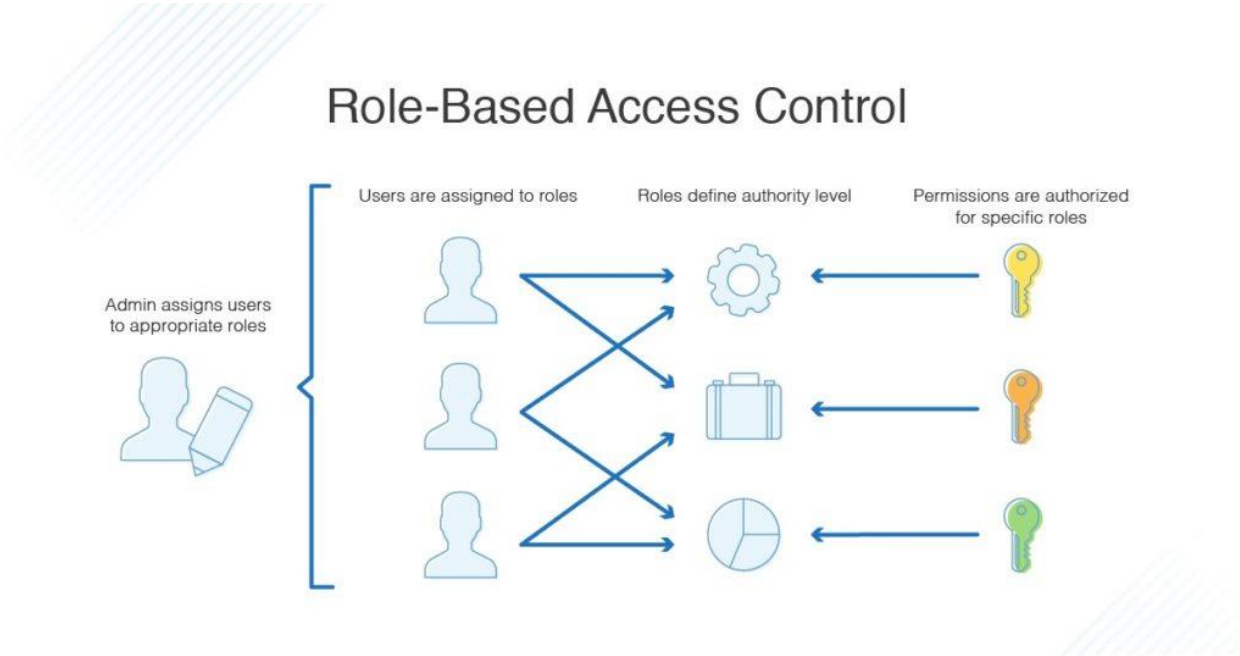

Figura 2.40. Controlul accesului bazat pe roluri

În controlul accesului bazat pe roluri, accesul este dat pe baza rolurilor acordate utilizatorului de administratorul ecosistemului cloud. Regulile de acces sunt definite prin politicile atribuite rolurilor. Exemple de roluri ar putea fi un rol pentru un dezvoltator care are nevoie de acces de citire și scriere la o bază de date și un rol pentru un contabil care are nevoie de acces la informațiile de facturare pentru aceeași bază de date. Ori de câte ori o persoană are nevoie de acces la resursele din roluri, utilizatorului i se poate atribui acel rol. Un utilizator poate avea, de asemenea, mai multe roluri atribuite, iar un rol poate avea mai mulți utilizatori asociați (vezi Figura 2.40.).

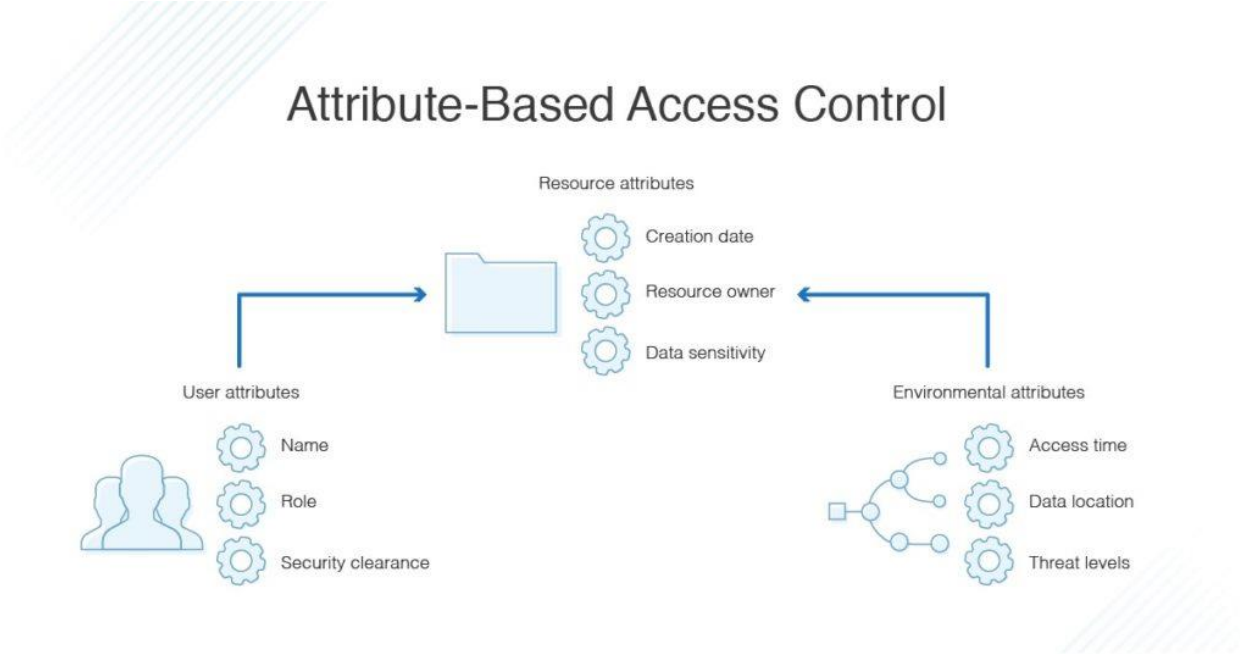

Figura 2.41. Controlul accesului bazat pe atribute

Într-un sistem de control al accesului bazat pe atribute, accesul la resurse este acordat utilizatorilor pe baza unor atribute definite în politica resursei. Acest lucru le permite utilizatorilor să creeze noi resurse la care utilizatorii autorizați au acces instantaneu, deoarece li s-a dat acces printr-un atribut, cum ar fi o etichetă. Aceasta înseamnă că administratorul nu trebuie să creeze sau să actualizeze politici pentru a permite accesul la noile resurse create (vezi Figura 2.41.).

RBAC vs ABAC – argumente pro și contra

ABAC argumente pro

- Nivel ridicat de control și granularitate
- Poate evita munca consumatoare de timp atunci când gestionați o cantitate copleșitoare de roluri

ABAC argumente contra

- Configurarea poate fi consumatoare de timp
- Trebuie implementat chiar de la început

RBAC argumente pro

- Direct și ușor de utilizat, reguli mai puțin complexe

RBAC argumente contra

- Poate duce la explozia de roluri când ar trebui să se gestioneze un număr excesiv de roluri diferite

Când să alegi un model RBAC?

- Companiile mici care gestionează puține resurse cloud și cu echipe mici unde există un risc mic de „explozie de rol”
- Dacă structura organizatorică este simplă și cu roluri bine definite.

Când să alegi un model ABAC?

- Dacă lucrați cu echipe temporare sau distribuite, la care poate fi necesar să acordați acces în funcție de locația din care accesează și de fusurile orare în care se află.
- Dacă există multă colaborare pe fișiere și documente, accesul trebuie să se bazeze mai degrabă pe tipul de document/fișier decât pe rolul care dorește să-l acceseze.

În multe cazuri, veți dori să aveți o combinație a ambelor modele în care RBAC oferă acces la un nivel superior, dar utilizați ABAC pentru a obține un control mai fin și mai granular.

2.3.4 Servicii de baze de date în cloud

La alegerea unei baze de date și a unui furnizor de baze de date există, ca și în cazul alegerii tipului de stocare/furnizorului de stocare, multe considerente diferite care trebuie luate în considerare. Există mai multe tipuri diferite de baze de date și toate au punctele lor forte și punctele slabe, în funcție de tipul de date care sunt stocate.

Bazele de date relaționale tradiționale care utilizează SQL (limbaj de interogare structurat), cum ar fi mySQL sau PostgreSQL, sunt excelente atunci când se lucrează cu seturi de date bine definite de la bun început și când nu vor exista modificări ale formatului datelor în timp, iar între diferitele părți ale setului de date există relații puternice și clare.

De exemplu, puteți avea o relație între o carte și o bibliotecă.
În acest caz, o bibliotecă va avea mai multe cărți, dar o carte nu poate aparține decât unei singure biblioteci (vezi Figura 2.42.).

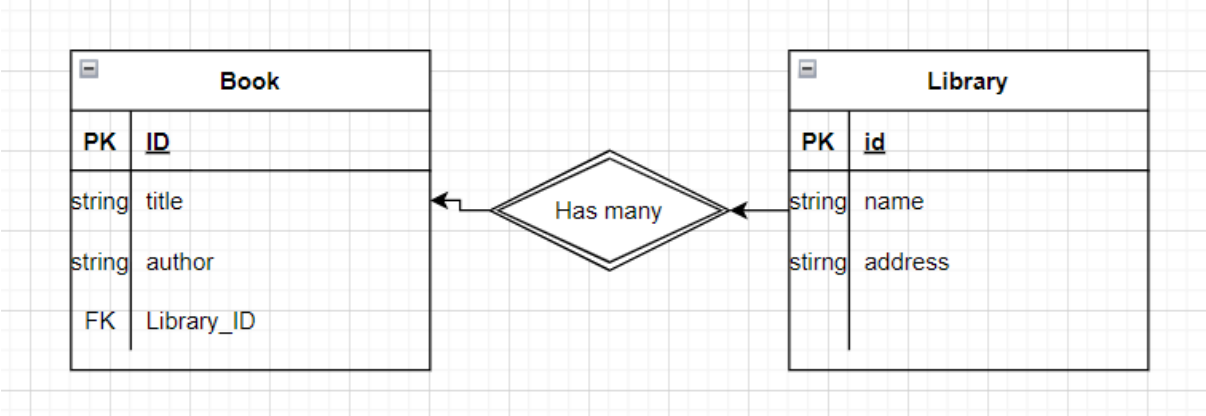

Figura 2.42. Relația dintre carte și bibliotecă

Dar, uneori, datele pe care le aveți nu sunt bine structurate și aveți mai puțin control asupra modului în care datele se vor schimba în timp. În aceste cazuri, cel mai bine ar fi să folosiți o bază de date NoSQL (nu numai SQL)....

Amazon RDS (Serviciul de baze de date relaționale) suportă o serie de baze de date relaționale dintre cele mai populare, cum ar fi mySQL, MariaDB și OracleSQL, dar oferă și propria bază de date relaționale numită Amazon Aurora.

Microsoft Azure oferă mai multe servicii de baze de date relaționale, cum ar fi Azure SQL Database, Azure Database pentru PostgreSQL/MariaDB/MySQL.

Google Cloud Platform are Cloud SQL, AlloyDB și Cloud Spanner. De asemenea, aceștia au o soluție optimizată pentru depozitele de date numită BigQuery.

Pentru soluțiile NoSQL, Google oferă propria bază de date de documente numită Firestore și o bază de date cu valori cheie numită Cloud Bigtable.

Microsoft Azure dispune de o soluție NoSQL numită Cosmos DB, care suportă o mare varietate de alte API-uri NoSQL, cum ar fi Apaches Cassandra și MongoDB, dar are și suport pentru SQL.

Serviciile NoSQL de la Amazon includ DocumentDB și DynamoDB, care sunt servicii gestionate

La alegerea tipului de bază de date și a furnizorului trebuie să se țină seama de anumite aspecte. Elementele cheie care trebuie luate în considerare sunt tipul de date care sunt stocate. Sunt datele foarte structurate, cu relații puternice? Cea mai bună alegere ar putea fi o bază de date relațională.

Pe lângă decizia privind tipul de bază de date care se potrivește cel mai bine, este important să se decidă ce clasă de instanță este necesară. Clasele de instanță DB determină cantitatea de memorie, CPU, debitul de I/O disponibil pentru serverul bazei de date.

Clasa de instanță DB: determină capacitatea de stocare a memoriei, a procesorului, a rețelei I/O - poate fi gestionat în consola de administrare AWS, AWS CLI, RDS API.

Securitatea BD: Proximitate la internet. - Cloud privat virtual. Gateway de rețea, control al accesului utilizează IAM, utilizatorii și rolurile pot fi utilizate pentru a determina accesul la acțiunile din BD (Obținerea, Înregistrarea).

AWS utilizează AES-256 în timpul repausului.
Zonele de disponibilitate Amazon pentru a crește durabilitatea în caz de defecțiune a infrastructurii.

O prezentare practică a modului de instanțiere a unei baze de date cu Amazon RDS utilizând Amazon Aurora MySQL (vezi Figura 2.43.):

Când vă aflați pe pagina principală a consolei aws, faceți clic pe butonul Services (Servicii) din stânga sus și apoi localizați "Database" (Bază de date) în meniul derulant. Faceți clic pe acesta și se va deschide un nou panou. Localizați "RDS" și faceți clic pe el.

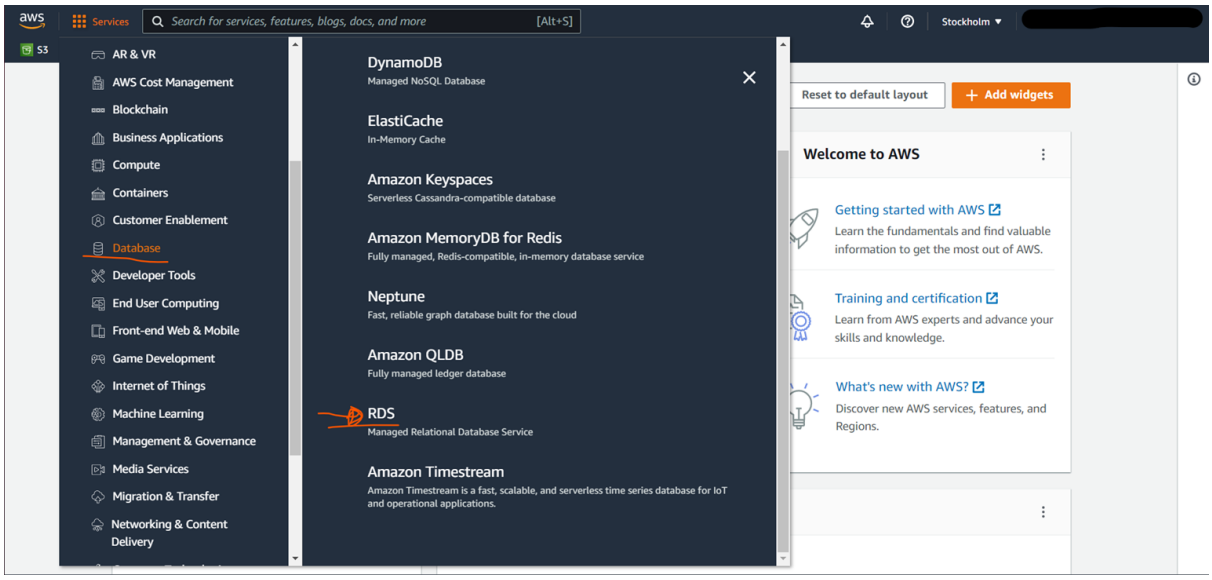

Figura 2.43. Baza de date cu Amazon RDS folosind Amazon Aurora MySQL

În pagina de pornire a consolei Amazon RDS, faceți clic pe Baze de date din meniul din stânga, ceea ce vă va duce la panoul cu prezentarea generală a tuturor bazelor de date conectate la contul dvs. AWS.

Pentru a crea o nouă bază de date, faceți clic pe butonul "Create database" (Creați o bază de date), care va deschide asistentul de creare a bazei de date (vezi Figura 2.44.).

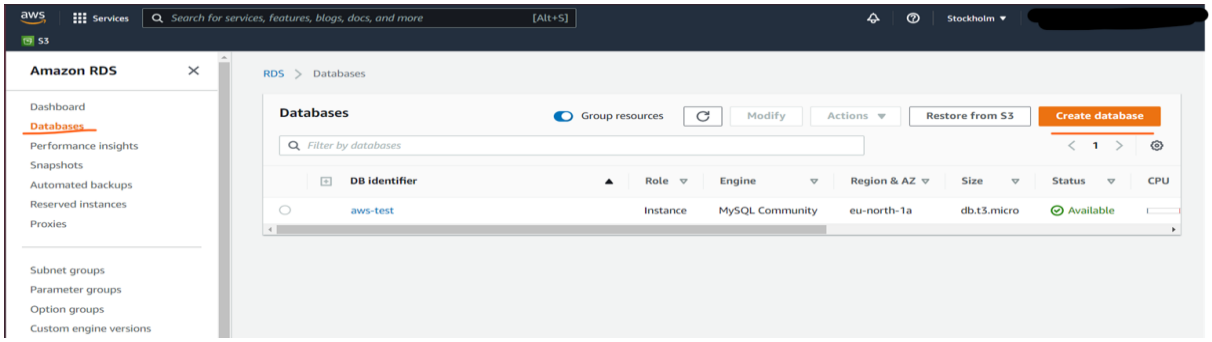

Figura 2.44. Creearea unei noi baze de date – primul pas

În cadrul asistentului veți avea mai multe opțiuni pentru baza de date relațională pe care doriți să o utilizați și, de asemenea, ce versiuni ale motoarelor de baze de date doriți să utilizați. Noi vom lăsa ca implicită alegerea ediției compatibile cu Amazon Aurora MySQL și vom face ca aceasta să ruleze pe versiunea MySQL 5.7 (vezi Figura 2.45.).

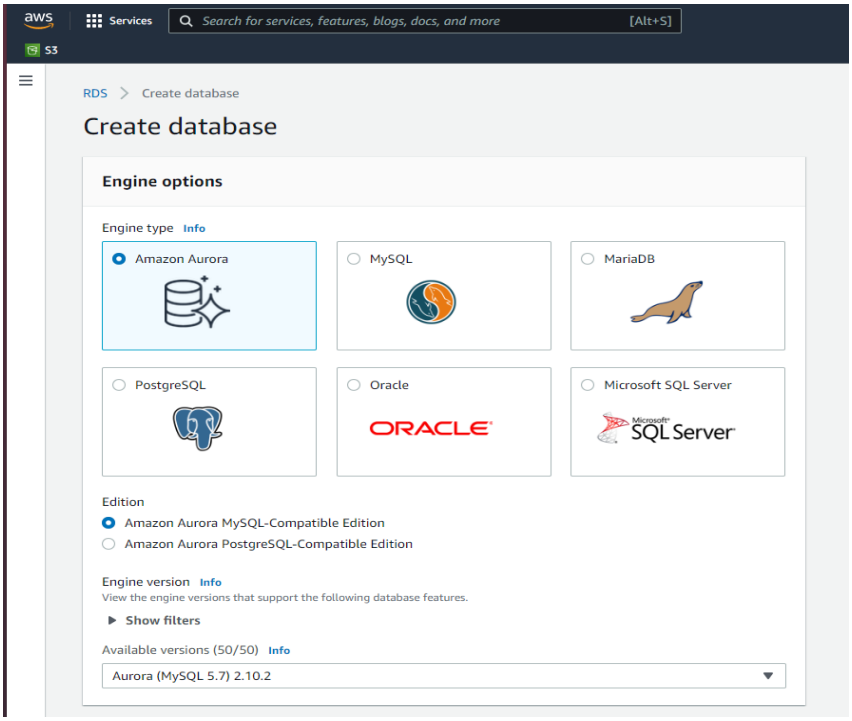

Figura 2.45. Creearea unei noi baze de date – pasul doi

Derulând în jos, putem impune setările pentru baza de date, definind numele clusterului (sau doar numele bazei de date, dacă se utilizează mysql) și datele de identificare, cum ar fi numele de utilizator și parola (vezi Figura 2.46.)

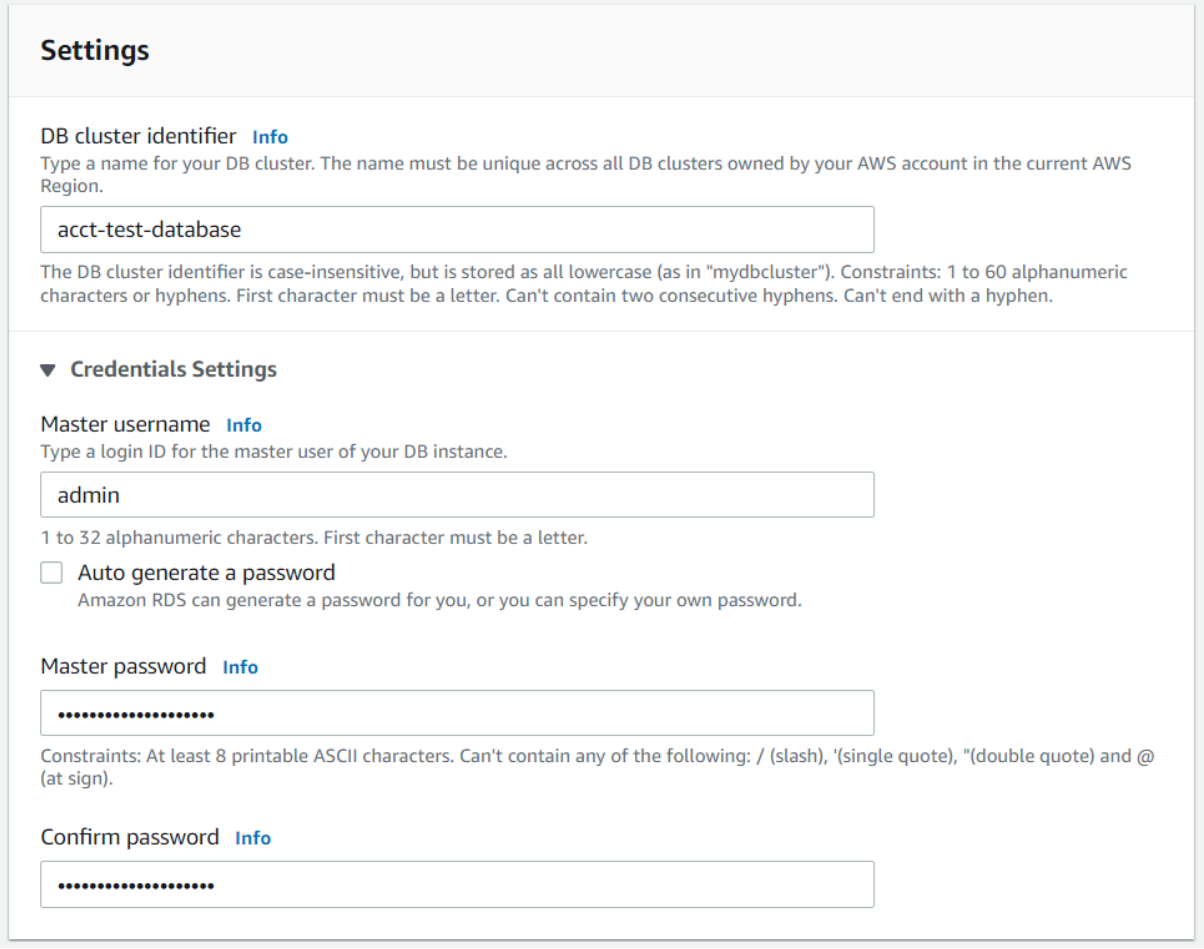

Figura 2.46. Setari ale bazei de date

În setarea de configurare a instanțelor, decideți ce clasă de instanță să utilizați pentru baza de date. În cazul nostru, vom alege clasa de instanță mai mică, care se poate sparge din motive de costuri, dar într-o aplicație reală ar trebui să se ia în considerare ce tip de seturi de date ar trebui să gestioneze, ce tip de modele de acces și ce tip de debit trebuie să poată gestiona.

Crearea unei replici Aurora poate fi aleasă pentru a crea replici în zone de disponibilitate diferite, astfel încât, dacă o AZ (Aurora Azure) se oprește sau întâmpină probleme, să puteți trece rapid la o altă AZ cu un timp de întrerupere minim (vezi Figura 2.47.).

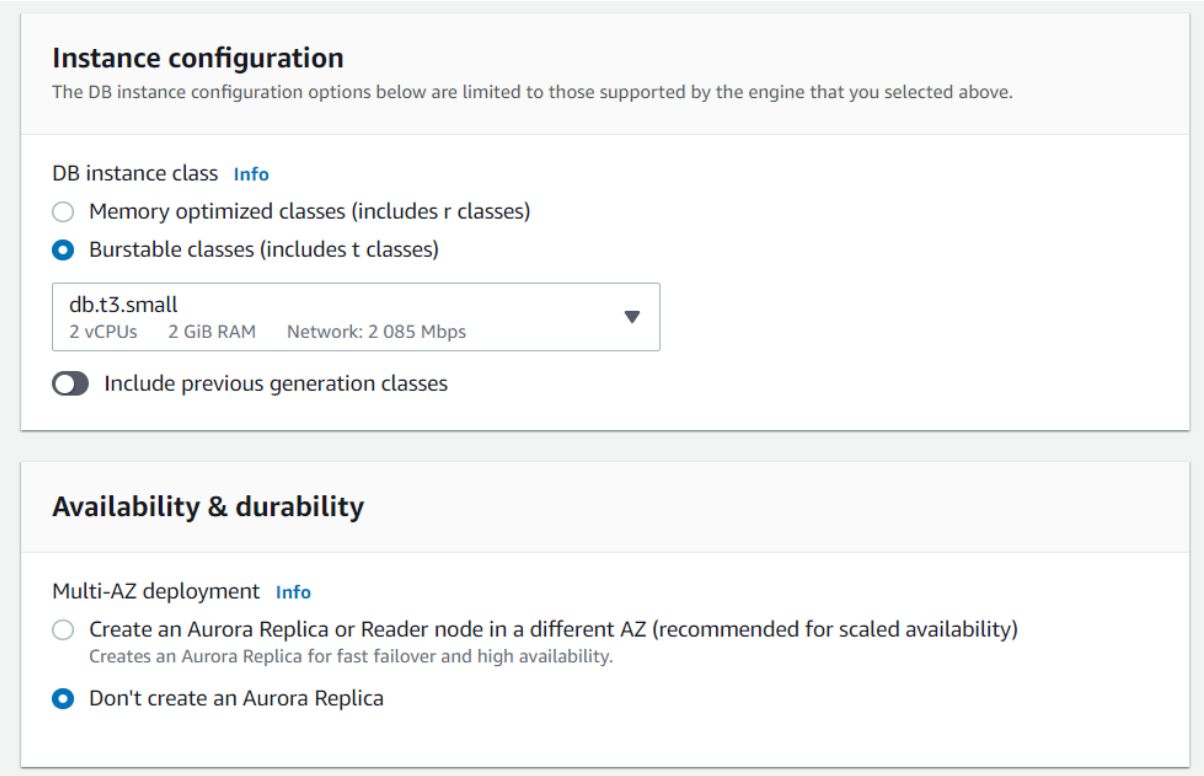

Figura 2.47. Crearea unei replici Aurora

În setările de conectivitate (vezi Figura 2.47.), veți stabili dacă doriți sau nu să vă conectați baza de date la Amazon Elastic Cloud Compute sau la o resursă EC2.

De asemenea, este necesar să se creeze un cloud privat virtual (VPC). În acest VPC puteți crea reguli speciale pentru cine are voie să acceseze resursa din cadrul acestuia.

Grupul de subrețele este utilizat pentru a defini ce IP-uri poate utiliza baza de date în cadrul VPC. Le vom lăsa ambele ca fiind implicite.

Accesul public definește dacă orice sau oricine care nu face parte din VPC poate accesa baza de date printr-o adresă IP publică creată de expertul. De obicei, doriți să dezactivați această opțiune, astfel încât numai resursele care se află în interiorul VPC să poată accesa baza de date, minimizând riscul de acces neautorizat.

Grupurile de securitate VPC sunt ca niște liste de acces pentru care adresele IP sunt autorizate să acceseze baza de date.

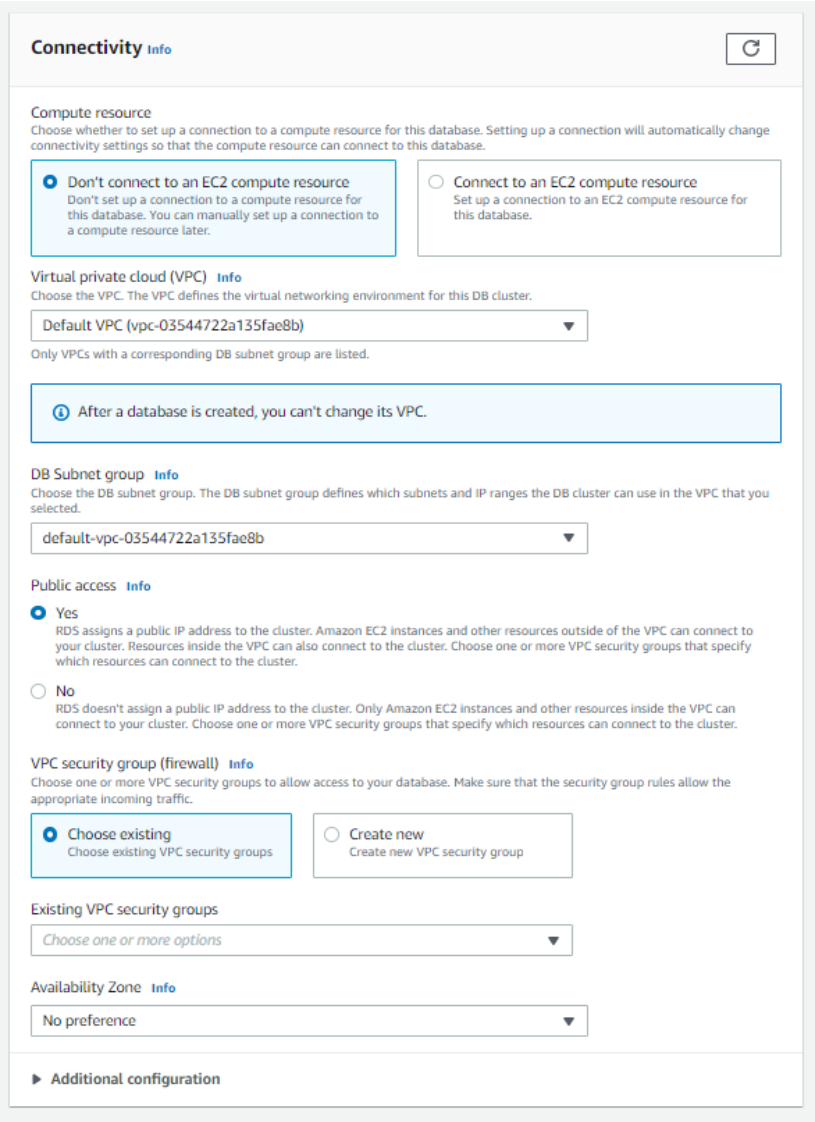

Figura 2.48. Setări de conectivitate

Puteți alege în ce zonă de disponibilitate din regiunea dvs. preferați să fie localizată baza de date

Autentificarea vă permite să decideți dacă este suficientă doar parola bazei de date sau dacă orice autentificare trebuie să includă și un utilizator/rol AWS IAM.

Monitorizarea urmărește utilizarea resurselor bazei de date. Acum că am configurat toate setările, putem crea baza de date. Faceți clic pe butonul de creare a bazei de date (vezi Figura 2.49.)

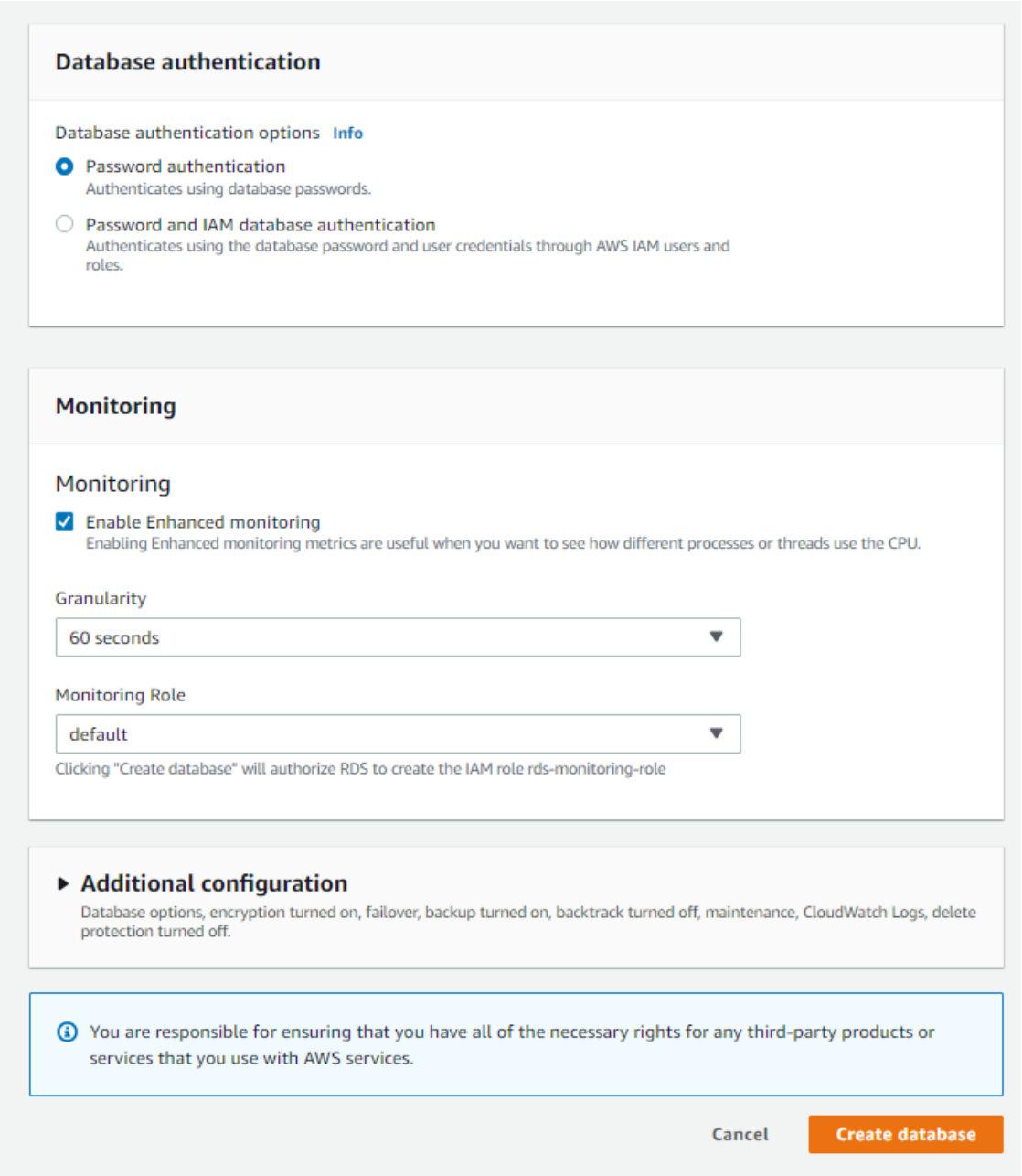

Figura 2.49. Crearea bazei de date

Baza noastră de date a fost creată și acum o putem vedea în lista din pagina de consolă Amazon RDS (vezi Figura 2.50.).

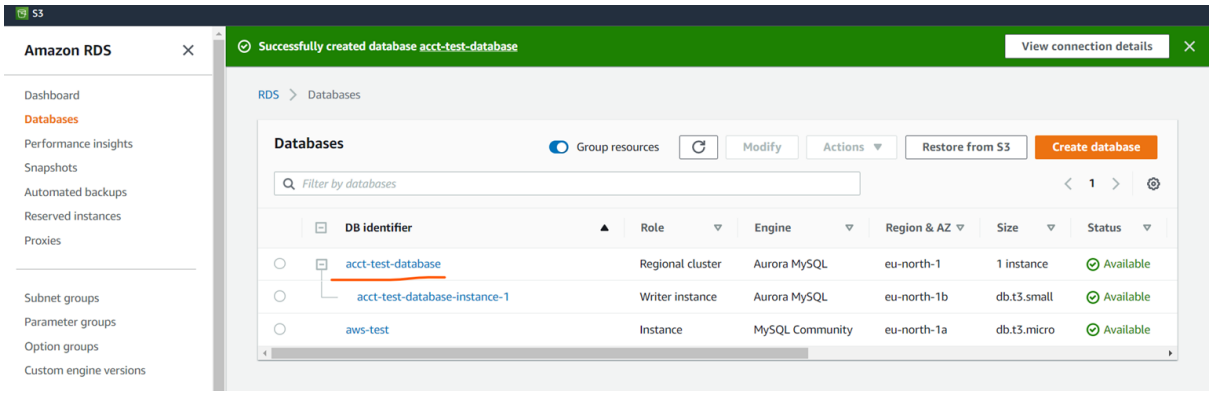

Figura 2.50. Baza de date creată vizibilă în pagina consolei Amazon RDS

Acum dacă am creat baza noastră de date, dorim să ne conectăm la ea și să creăm câteva tabele. Dând clic pe numele bazei de date pe care tocmai am creat-o, putem vedea punctul final al bazei de date (vezi Figura 2.51.). Aceasta este adresa la care trebuie să ne conectăm.

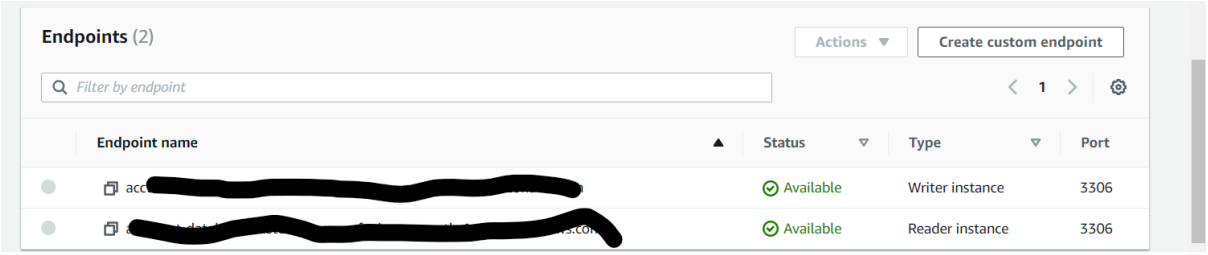

Figura 2.51 .Punctele finale ale bazei de date create

În continuare, vom folosi MySQL workbench pentru a ne conecta la această bază de date.Făcând clic pe semnul plus încercuit de lângă locul unde scrie "Conexiuni MySQL", se va deschide fereastra din imagine.Numele de gazdă este locul unde veți lipi punctul final de pe server, iar numele de utilizator va fi numele de utilizator al bazei de date principale pe care l-ați ales atunci când ați creat baza de date. După ce ați furnizat aceste două date, puteți face clic pe "test connection". Apoi vi se va cere să furnizați parola pe care ați setat-o. Dacă totul funcționează, veți primi un mesaj care vă va spune că s-a realizat o conexiune. Puteți apoi să dați un nume conexiunii și să faceți clic pe OK.

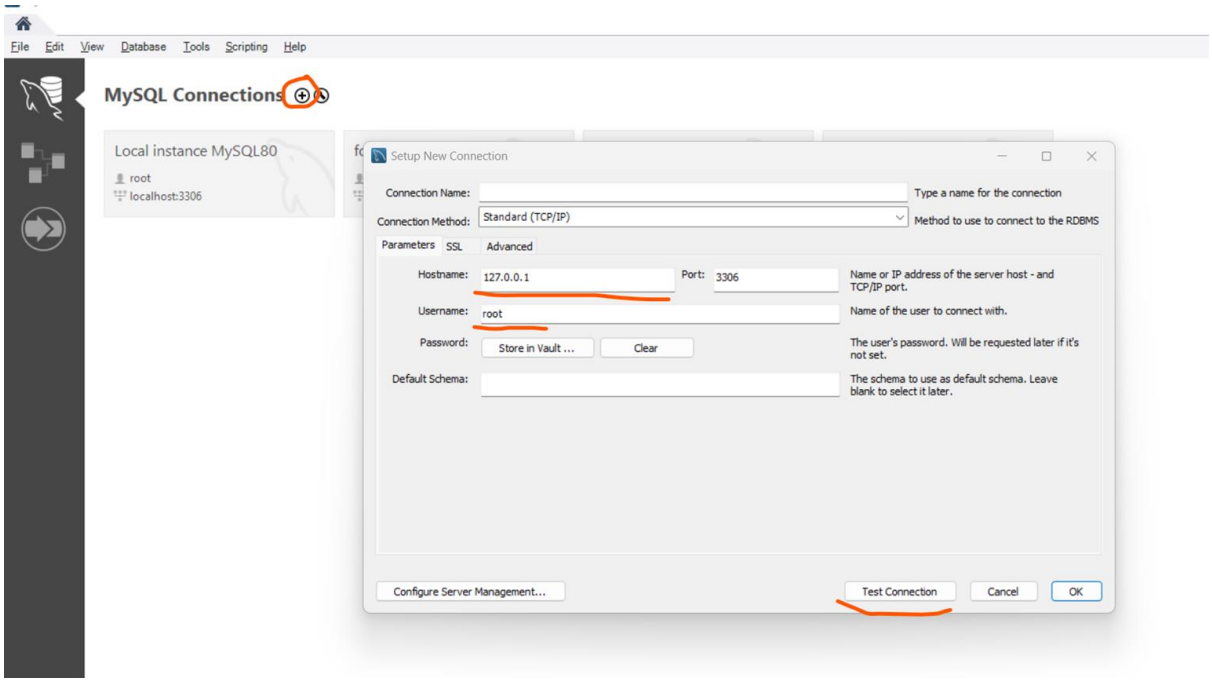

Figura 2.52. Utilizarea workbench-ului MySQL pentru conectarea la noua bază de date

După ce vă conectați cu succes la baza de date și vă autentificați, veți putea începe să creați baze de date cu tabele și informații folosind instrucțiuni SQL.

2.3.5 Considerații pentru configurarea domeniului

În această unitate veți învăța că, atunci când aleg furnizorul potrivit de servicii cloud, companiile ar trebui să ia în considerare mai mult decât doar suite de produse. Aproape toate companiile folosesc un furnizor de infrastructură ca serviciu (IaaS) sau platformă ca serviciu (PaaS). Este posibil ca organizațiile să înceapă cu unul dintre cei trei furnizori de cloud, Amazon Web Services (AWS), Azure sau Google Cloud Platform (GCP) și pot decide să reducă riscul oferind o bază diversă de servicii prin mai mulți furnizori, să optimizeze prin implementarea sarcinilor de lucru potrivite în cloud și minimizați blocarea furnizorilor.

Diferențele cheie între platformele cloud

1. O privire asupra Amazon Web Services (AWS)

Când AWS a fost lansat pentru prima dată în 2006, a furnizat în principal servicii de calcul, stocare și baze de date utilizate de dezvoltatori. Fiind primul furnizor de cloud, AWS rămâne inovator, deoarece a avut o bază anterioară pe care să se construiască.

Majoritatea companiilor folosesc următoarele servicii pe AWS:

- AWS Elastic Compute Cloud (EC2):scalabil, putere de calcul scalabilă pentru găzduirea de software sau învățarea automată
- AWS Relational Database Service (RDS): un motor de baze de date personalizabil pentru găzduirea serverelor de baze de date și lucrul cu baze de date NoSQL.
- AWS Lambda Functions as a Service (FaaS): calcul fără server bazat pe evenimente pentru procese de fundal, cum ar fi transformarea imaginilor, procesarea datelor în timp real și validarea datelor în flux.
- AWS Simple Storage Service (S3): inițial pentru dezvoltatori cu stocare persistentă, dar și pentru arhivare și migrare rentabilă a datelor
- AWS Elastic Container Service (ECS): Gestionarea containerelor pentru pornirea, oprirea și gestionarea containerelor cluster.
- AWS CloudFront Content Delivery Network (CDN): Stochează date la margine pentru a furniza date, videoclipuri, imagini, aplicații și API-uri.

2. Ce oferă Azure?

Azure tinde să promoveze organizațiile tip întreprinderi care au investit deja în produse și servicii Microsoft

- Majoritatea companiilor Azure folosesc următoarele servicii:
- Azure Hybrid: un serviciu pentru încărcături de lucru care combină licențe Windows Server și SQL Server la nivel local
- Azure Virtual Desktop (AVD): Virtual Desktop Interface (VDI) pentru acces de la distanță la Windows 10 și aplicații
- Azure Sentinel: Security Information Event Management (SIEM) și Security Orchestration Automated Response (SOAR) pentru detectarea, vizibilitatea și răspunsul la amenințări
- Azure Cosmos DB: bază de date NoSQL cu API deschisă pentru aplicații mobile/web, jocuri și comerț electronic/retail
- Azure Active Directory (AD): un serviciu de identitate care se sincronizează în mediile Microsoft on-premises și cloud cu conectare unică și autentificare cu mai mulți factori.

3. Google Cloud Platform (GCP) și cum se compară

Pentru a nu fi mai prejos, Google a lansat o versiune beta a GCP în 2008. În timp ce AWS oferă servicii IaaS, GCP sa concentrat inițial pe serviciile PaaS. Dezvoltatorii își pot dezvolta și rula aplicațiile web în centre de date gestionate de Google. De-a lungul timpului, GCP și-a extins ofertele pentru a include suite Google, tehnologii de date mari și instrumente de management.

GCP se concentrează în general pe dezvoltatorii care doresc să creeze și să ruleze aplicații. Tinde să se concentreze pe organizațiile care doresc să creeze aplicații, dar nu au centrele de date locale care să le susțină. Majoritatea companiilor folosesc următoarele servicii în GCP:

- Google Compute Engine: o mașină virtuală bazată pe nucleu (KVM) preconfigurată sau personalizabilă pentru serverele Linux și Microsoft
- Google Cloud Storage (GCS): stocare bloc, fișiere și obiecte cu reguli de gestionare a ciclului de viață pentru diferite tipuri de date
- Google Kubernetes Engine (GKE): un mediu de pregătire gestionat, gestionat pentru implementarea microserviciilor
- BigQuery Machine Learning (ML): Modele de Machine Learning pentru perspective de afaceri.

Câte regiuni de disponibilitate are fiecare furnizor?
Acest lucru este important atunci când se determină cerințele de conformitate ale unei companii, care, conform Regulamentului general privind protecția datelor (GDPR), companiile ar trebui să stocheze și să proceseze date într-una dintre țările UE.
Iată cum se clasează concurenții:

- AWS: 26 de regiuni geografice
- Azure: peste 60 de regiuni
- GCP: 29 de regiuni

De obicei, fiecare regiune are mai multe zone de disponibilitate. Aceasta înseamnă că ar trebui să luați în considerare următoarele:

- AWS: 84 de zone de disponibilitate în total
- Azure: 3 zone de disponibilitate per regiune, cel puțin 180 în total
- GCP: 88 de zone de disponibilitate

Considerațiile suplimentare pot include opțiuni de servicii specializate pe care le are fiecare furnizor și care diferă:

- AI/învățare automată
- Internetul lucrurilor (IoT)
- Realitate augmentată/realitate virtuală
- analiza afacerii
- tehnologia robotului

Structura prețurilor
Fiecare dintre cei trei furnizori mari oferă modele de prețuri diferite bazate pe utilizarea cloud de către o organizație. Toți cei trei furnizori consideră că stabilirea prețurilor și facturarea sunt dificile, ceea ce înseamnă că trebuie să fiți conștient de următoarele atunci când vă gândiți ce server să utilizați:

- Guvernare
- Format de facturare
- Monitorizați consumul și bugetul
- Modificări ale modelului de prețuri
- Valoarea prețului pe termen lung comparativ cu plata pe măsură

Instrumente de management

După cum s-a menționat deja, puteți utiliza diferite servicii cloud pentru a combina resurse și instrumente pentru a eficientiza și centraliza nevoile de afaceri. Cu toate acestea, este important de reținut că AWS și Azure sunt mai orientate spre afaceri decât GCP, iar AWS oferă cea mai mare gamă de servicii externalizate. Aceasta poate fi o considerație majoră pentru acele companii care au nevoie de cele mai solide opțiuni (vezi Figura 2.53.). Lată un grafic care detaliază diferențele.

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

Figura 2.53. Lista cu diferite servicii cloud

De asemenea,cheia pentru gestionarea serviciilor, care sunt cele care utilizează instrumente IoT și cum diferă acestea(vezi Figura 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

Figura 2.54. Servicii de management, care utilizează instrumente IoT

Întrebări de luat în considerare:

- Care sunt principalele diferențe între cele trei servere și ce platformă ar fi mai atrăgătoare pentru un început de afaceri față de unul cu nevoi de management foarte puternice?
- Ce fel de structură a prețurilor v-ar atrage cel mai mult din perspectiva dvs. actuală?
- În același sens, cum v-ar afecta acoperirea regională alegerea?
- Citiți acest articol și luați în considerare care sunt principalele dvs. considerații ca proprietar de afaceri actual sau potențial atunci când vă decideți asupra unei platforme?

https://www.netsolutions.com/insights/how-to-choose-cloud-service-provider/

Resurse adiționale: Samoshkin (n. d.), Cloud Industry Forum (2022), Rathore (2022), CloudSigma (2023).

2.4 Tipuri de conectivitate ale serviciilor de rețea și setarea lor

2.4.1 Despre arhitectura cloud

Termenul "cloud" pare să își aibă originile în diagramele de rețea care reprezentau internetul, sau diverse părți ale acestuia, sub forma unor nori schematici. "Cloud computing" a fost inventat pentru ceea ce se întâmplă atunci când aplicațiile și serviciile sunt mutate în "norul" internetului. Cloud computing nu este ceva care a apărut brusc peste noapte; într-o anumită formă, poate fi privit in urmă până la o perioadă în care sistemele de calculatoare împărțeau la distanță resurse și aplicații de calcul

în timp real. Totuși, în prezent, "cloud computing" se referă la numeroasele tipuri diferite de servicii și aplicații care sunt furnizate în "norul" internetului și la faptul că, în multe cazuri, dispozitivele utilizate pentru a accesa aceste servicii și aplicații nu necesită aplicații speciale.

Întreprinderile caută adesea să găsească cea mai bună soluție cloud care să se potrivească nevoilor lor organizaționale unice. O mare parte din această decizie este selectarea unui furnizor de servicii cloud. Există patru furnizori principali de servicii cloud care controlează majoritatea resurselor cloud globale. Cu toate acestea, există și alte soluții cloud mai puțin cunoscute, care oferă servicii specifice unor piețe de nișă.

Cei patru furnizori de servicii de cloud computing, cei mai utilizați, oferă toți SaaS, PaaS, IaaS și multe alte servicii de cloud computing la scară globală. Principalii furnizori de servicii cloud sunt:

- Servicii Google Cloud
- Microsoft Azure
- Servicii Web Amazon (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.

Figura 2.55. Prezentare generală a serviciilor

Printre alte soluții cloud care oferă servicii specifice se numără următoarele:

- Heroku: Furnizor important de servicii PaaS în cloud, inclusiv dezvoltarea, implementarea, gestionarea și scalarea aplicațiilor.
- GitHub: Un serviciu de depozit de control al versiunilor de mari dimensiuni utilizat pentru dezvoltarea colaborativă de aplicații. Dezvoltatorii și managerii pot revizui codul, pot gestiona proiecte și pot construi software ca efort comun.

- **QuickBooks Online:** Versiunea SaaS a programului de contabilitate oferit de QuickBooks.
- **BackBlaze:** Oferă un serviciu cloud de backup și recuperare a datelor pentru uz personal și de afaceri.
- **ClearDATA:** Oferă soluții cloud specifice industriei de sănătate. Concepute pentru a ajuta instituțiile să respecte reglementările din domeniu.
- **Salesforce.com**: Își execută setul de aplicații pentru clienții săi într-un cloud, iar produsele sale Force.com și Vmforce.com oferă dezvoltatorilor platforme pentru a construi servicii cloud personalizate.

Aceasta este doar o mică prezentare a diverselor soluții cloud disponibile. Cu toate acestea, acești furnizori de servicii cloud oferă o bază solidă pentru a înțelege ce fel de servicii sunt disponibile.

Caracteristici

Cloud computing are o varietate de caracteristici, dintre care principalele sunt:

- **Infrastructură** partajată - Folosește un model software virtualizat, permițând partajarea serviciilor fizice, a capacităților de stocare și de rețea. Infrastructura cloud, indiferent de modelul de implementare, urmărește să valorifice la maximum infrastructura disponibilă pentru un număr de utilizatori.
- **Aprovizionare dinamică** - Permite furnizarea de servicii pe baza cerințelor actuale ale cererii. Acest lucru se realizează în mod automat cu ajutorul automatizării software-ului, permițând extinderea și contractarea capacității de servicii, în funcție de necesități. Această scalare dinamică trebuie să se facă menținând în același timp un nivel ridicat de fiabilitate și securitate.
- **Accesul la rețea** - Trebuie să fie accesat pe internet de pe o gamă largă de dispozitive, cum ar fi PC-uri, laptopuri și dispozitive mobile, utilizând API-uri bazate pe standarde (de exemplu, cele bazate pe HTTP). Implementările de servicii în cloud includ orice, de la utilizarea aplicațiilor de afaceri la cea mai recentă aplicație pe cele mai noi smartphone-uri.
- **Contorizare gestionată** - Utilizează contorizarea pentru gestionarea și optimizarea serviciului și pentru a furniza informații de raportare și facturare. În acest fel, consumatorii sunt facturați pentru servicii în funcție de cât au folosit efectiv în perioada de facturare.

Pe scurt, cloud computing permite partajarea și implementarea scalabilă a serviciilor, în funcție de necesități, din aproape orice locație, pentru care clientul poate fi facturat în funcție de utilizarea reală.

Modele de servicii

Odată ce un cloud este stabilit, modul în care sunt implementate serviciile de cloud computing în ceea ce privește modelele de afaceri poate diferi în funcție de cerințe. Principalele modele de servicii care sunt desfășurate (a se vedea Figura 2.56.) sunt cunoscute în mod obișnuit sub denumirea de:

- **Software as a Service (SaaS)** - Consumatorii achiziționează posibilitatea de a accesa și utiliza o aplicație sau un serviciu găzduit în cloud. Un exemplu de referință în acest sens este Salesforce.com, după cum s-a discutat anterior, unde informațiile necesare pentru interacțiunea dintre consumator și

serviciu sunt găzduite ca parte a serviciului în cloud. De asemenea, Microsoft a făcut o investiție semnificativă în acest domeniu și, ca parte a opțiunii de cloud computing pentru Microsoft® Office 365, suita sa Office este disponibilă sub formă de abonament prin intermediul serviciilor sale online bazate pe cloud.

- Platform as a Service (PaaS) - Consumatorii achiziționează acces la platforme, ceea ce le permite să își implementeze propriile programe și aplicații în cloud. Sistemele de operare și accesul la rețea nu sunt gestionate de către consumator și pot exista constrângeri în ceea ce privește aplicațiile care pot fi implementate. Printre exemple se numără Amazon Web Services (AWS), Rackspace și Microsoft Azure.
- Infrastructură ca serviciu (IaaS) - Consumatorii controlează și gestionează sistemele în ceea ce privește sistemele de operare, aplicațiile, spațiul de stocare și conectivitatea rețelei, dar nu controlează ei înșiși infrastructura cloud.

Aplicația utilizatorului final este furnizată ca serviciu. Platforma și infrastructura sunt abstracte și pot fi implementate și gestionate cu mai puțin efort. Platforma de aplicații pe care pot fi implementate aplicații și servicii. Se poate construi și implementa mai ieftin, deși serviciile trebuie să fie susținute și gestionate. Infrastructura fizică este abstractizată pentru a furniza servicii de calcul, stocare și rețea, evitând cheltuielile și nevoia de sisteme dedicate.

Figura 2.56. Tipuri de modele de servicii

Modele de implementare

Implementarea cloud computing-ului poate fi diferită în funcție de cerințe și au fost identificate următoarele patru modele de implementare, fiecare cu caracteristici specifice care susțin nevoile serviciilor și ale utilizatorilor de cloud-uri în moduri specifice (a se vedea Figura 2.57.).

- Cloud privat - Infrastructura cloud a fost implementată, este întreținută și operată pentru o anumită organizație. Operarea poate fi internă sau cu o terță parte în incintă.
- Cloud comunitar - Infrastructura cloud este împărțită între mai multe organizații cu interese și cerințe similare. Acest lucru poate contribui la limitarea costurilor de investiții pentru înființarea sa, deoarece costurile sunt împărțite între organizații. Operarea poate fi internă sau cu o terță parte în incintă.
- Cloud public - Infrastructura cloud este pusă la dispoziția publicului pe bază comercială de către un furnizor de servicii cloud. Acest lucru permite unui consumator să dezvolte și să implementeze un serviciu în cloud cu un efort financiar foarte mic în comparație cu cerințele de cheltuieli de capital asociate în mod normal cu alte opțiuni de implementare.

- **Cloud hibrid** - Infrastructura cloud este formată dintr-un număr de cloud-uri de orice tip, dar cloud-urile au capacitatea, prin intermediul interfețelor lor, de a permite mutarea datelor și/sau a aplicațiilor dintr-un cloud în altul. Aceasta poate fi o combinație de cloud-uri private și publice care să susțină cerința de a păstra unele date într-o organizație și, de asemenea, nevoia de a oferi servicii în cloud.

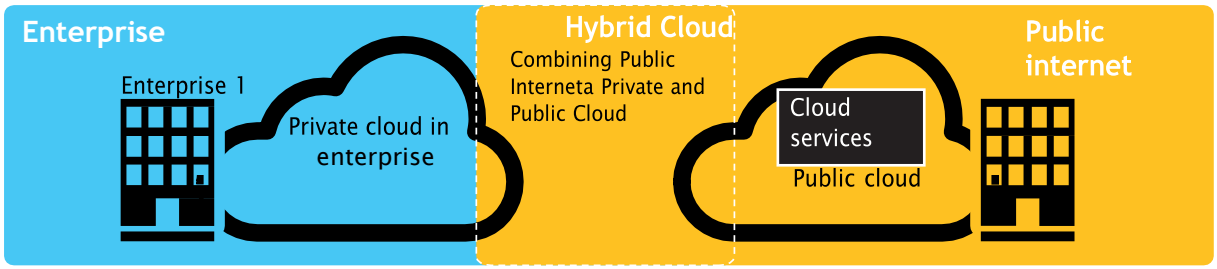

Figura 2.57. Exemplu de implementare a cloud-ului public, privat și hibrid

Provocari

Următoarele sunt câteva dintre provocările notabile asociate cu cloud computing și, deși unele dintre acestea pot cauza o încetinire a furnizării mai multor servicii în cloud, majoritatea pot oferi, de asemenea, oportunități, dacă sunt rezolvate cu atenția și grija cuvenite în etapele de planificare.

- **Securitate și confidențialitate -** Probabil că două dintre cele mai "fierbinți" probleme legate de cloud computing se referă la stocarea și securizarea datelor și la monitorizarea utilizării cloud-ului de către furnizorii de servicii. În general, acestor probleme li se atribuie încetinirea implementării serviciilor de cloud computing. Aceste provocări pot fi abordate, de exemplu, prin stocarea informațiilor în interiorul organizației, dar permițând ca acestea să fie utilizate în cloud. Totuși, pentru ca acest lucru să se întâmple, mecanismele de securitate dintre organizație și cloud trebuie să fie solide, iar un cloud hibrid ar putea sprijini o astfel de desfășurare.
- **Lipsa standardelor -** Cloudurile au interfețe documentate; cu toate acestea, nu există standarde asociate cu acestea și, prin urmare, este puțin probabil ca majoritatea cloud-urilor să fie interoperabili. Open Grid Forum dezvoltă o interfață deschisă de cloud computing pentru a rezolva această problemă, iar Open Cloud Consortium lucrează la standarde și practici de cloud computing. Cu toate acestea, menținerea la curent cu cele mai recente standarde, pe măsură ce acestea evoluează, va permite valorificarea lor, dacă este cazul.
- **Evoluție continuă -** Cerințele utilizatorilor sunt în continuă evoluție, la fel ca și cerințele privind interfețele, rețelele și stocarea. Acest lucru înseamnă că un "cloud", în special unul public, nu rămâne static și, de asemenea, evoluează continuu.
- **Preocupări legate de conformitate** - UE are un suport legislativ pentru protecția datelor în toate statele membre, dar în SUA protecția datelor este diferită și poate varia de la un stat la altul. La fel ca în cazul securității și confidențialității menționate anterior, acestea au ca rezultat, de obicei, implementarea cloud-ului hibrid, cu un cloud care stochează datele interne ale organizației.

2.4.2 Principii de conectivitate ale accesului la cloud

Pentru dezvoltatorii de servicii, punerea la dispoziție a serviciilor în cloud depinde de tipul de serviciu și de dispozitivul (dispozitivele) utilizat(e) pentru a-l accesa. Procesul poate fi la fel de simplu ca un utilizator care face clic pe pagina web necesară sau poate implica o aplicație care utilizează un API pentru a accesa serviciile din cloud.

Accesarea prin API-uri web

Accesul la capacitățile de comunicare într-un mediu bazat pe cloud se realizează prin intermediul API-urilor, în principal API-uri RESTful Web 2.0, care permit dezvoltatorilor de aplicații din afara cloud-ului să profite de infrastructura de comunicare din cadrul acestuia (a se vedea Figura 2.58.).

Aceste API-uri deschid o serie de posibilități de comunicare pentru serviciile bazate pe cloud, limitate doar de capacitățile de media și de semnalizare din cadrul cloud-ului. Serviciile media actuale permit comunicarea și gestionarea comunicațiilor vocale și video într-o gamă complexă de codecuri și tipuri de transport.

Prin utilizarea API-urilor web, aceste complexități pot fi simplificate, iar suportul media poate fi livrat mai ușor către dispozitivul la distanță. API-urile permit, de asemenea, comunicarea altor servicii, oferind noi oportunități și contribuind la creșterea venitului mediu pe utilizator (ARPU) și a ratelor de conectare, în special pentru operatorii de telecomunicații.

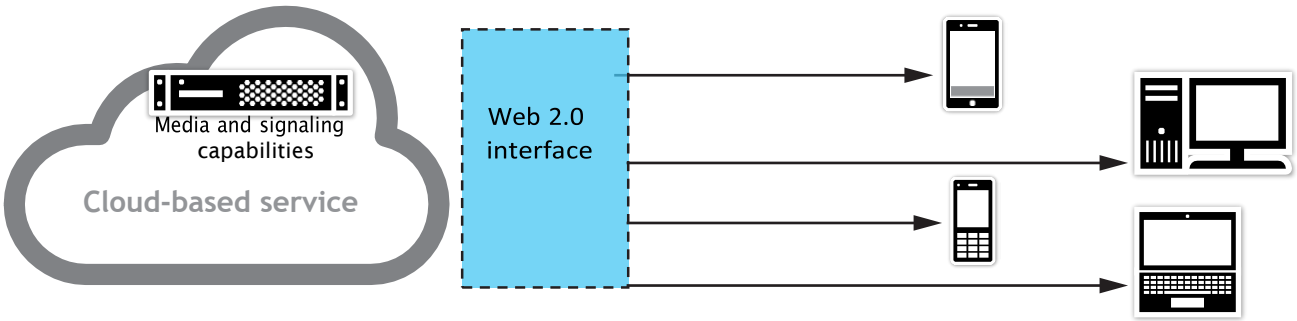

Figura 2.58. Interfețe Web 2.0 pentru cloud

Scalabilitatea comunicațiilor

Pentru a îndeplini cerințele de scalabilitate pentru implementările bazate pe cloud, software-ul de comunicații ar trebui să fie capabil să funcționeze în medii virtuale. Acest lucru permite creșterea și reducerea cu ușurință a densității sesiunilor în funcție de nevoile din acel moment, menținând în același timp la minimum necesarul de resurse fizice pe servere.

Selectarea opțiunii de conectivitate în cloud

Mulți furnizori de servicii de rețea (NSP) dispun de o gamă largă de opțiuni în ceea ce privește conectivitatea în cloud, deși lipsa standardelor din industrie și terminologia confuză pot face ca lucrurile să fie dificil de înțeles.

Nu cu mult timp în urmă, singura opțiune disponibilă pentru conectarea la un furnizor de servicii cloud (CSP) era prin intermediul internetului public. Cu toate acestea, odată cu trecerea rapidă la cloud computing, clienții au început rapid să ceară mai mult - securitate mai bună, latență mai mică, debite mai mari și fiabilitate sporită.

Furnizorii de servicii de comunicații sociale și-au dat seama în curând că o performanță mai bună a cloud-ului de la un capăt la altul nu va fi posibilă folosind internetul public. De asemenea, au înțeles că nu aveau expertiza sau infrastructura necesară pentru a gestiona interconectivitatea între zeci de furnizori de servicii de rețea și rafturile de colocare din propriile centre de date.

De asemenea, furnizorii de servicii de comunicații sociale și-au dat seama rapid că răspunsul se afla în sutele de centre de date neutre pentru operatorii de telefonie mobilă răspândite în întreaga lume, cunoscute și sub numele de puncte de schimb de internet (sau IXP). Toți furnizorii de servicii de rețea erau deja prezenți în aceste locații, astfel încât furnizorii de servicii de comunicații sociale puteau să-și extindă conectivitatea backbone pentru a se întâlni cu ei acolo. Acest lucru a oferit posibilitatea unei legături fizice directe între rețeaua furnizorului de servicii de rețea și rețeaua furnizorului de servicii cloud (cunoscută sub numele de cross-connect), ocolind internetul obișnuit și oferind o rețea pseudo-privată. Această interconectivitate, cunoscută sub numele de peering privat, a permis conectivitatea directă, de la un capăt la altul, și a adus cu ea o serie întreagă de îmbunătățiri în materie de securitate, latență și performanță (pe lângă eficientizarea costurilor pentru clienții care mută volume mari de date din mediile cloud în locațiile lor).

În prezent, conectivitatea în cloud se împarte în două categorii: una care se bazează pe internetul public și alta care utilizează conectivitate privată, dedicată. În cadrul acestor două categorii sunt disponibile, de obicei, 5 opțiuni de conectivitate diferite (vezi Figura 2.59.).

Conectivitate la internet	Conectivitate dedicată
Internet public	Ethernet
Internet public cu prioritizare cloud	MPLS IP VPN
	SD WAN

Figura 2.59. Conectivitate pentru cloud

Vom face o incursiune printre cele 5 opțiuni de conectivitate în cloud și vă vom explica avantajele și dezavantajele fiecăreia, astfel încât să puteți alege cea mai potrivită soluție de acces în cloud pentru nevoile dumneavoastră (vezi Figura 2.60.).

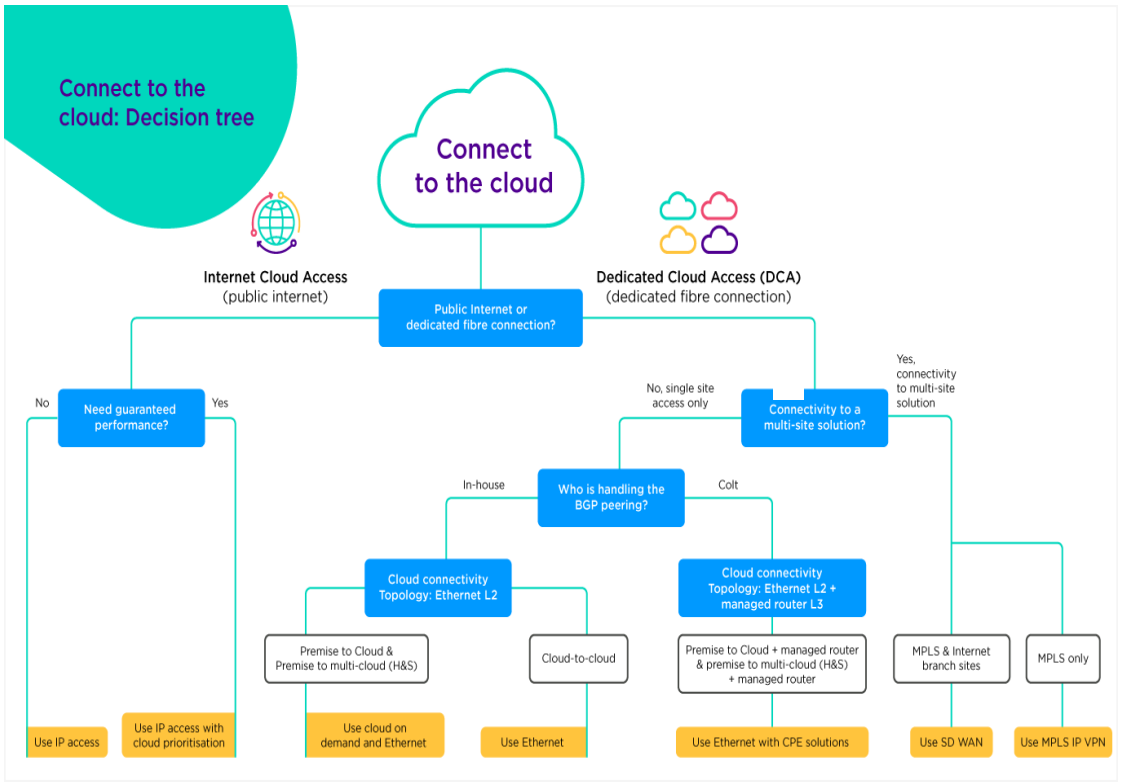

Figura 2.60. Conectarea la cloud - arborele de decizie

Conectivitate în cloud folosind internetul public

După cum se poate demonstra cea mai ieftină și mai ușoară modalitate de a vă conecta la cloud este prin intermediul conexiunii standard la internet prin intermediul internetului public, denumită uneori acces IP sau tranzit IP.

Utilizarea accesului public la internet este ușor de configurat și versatilă, deoarece accesul la cloud este doar unul dintre numeroasele cazuri de utilizare a unei conexiuni standard de acces la internet. Este o metodă de acces eficientă din punct de vedere al costurilor atunci când nu aveți nevoi specifice de performanță.

Cu toate acestea, accesarea aplicațiilor în cloud prin intermediul internetului public poate duce, de asemenea, la inconsecvențe în ceea ce privește performanța și la creșterea riscurilor de securitate. Din punct de vedere istoric, termenul de tranzit IP a fost utilizat pentru a reflecta situațiile în care furnizorii nu aveau acces direct la rețeaua de destinație și trebuiau să "tranziteze" alte rețele și alți furnizori de rețele.

Vă puteți gândi la rutele publice de internet ca la o autostradă - acestea sunt dinamice și partajate, ceea ce poate duce uneori la congestie, iar atunci când cea mai directă legătură nu este disponibilă, datele sunt direcționate prin următoarea cea mai bună opțiune, asupra căreia nu aveți niciun control, ceea ce duce la pierderea de pachete și la creșterea latenței (întârzierilor). În plus, transferurile multiple între furnizorii de servicii de internet creează instabilitate în conexiune și riscuri sporite.

În esență, cu cât sunt mai multe pop-up-uri și routere implicate în livrarea datelor dumneavoastră la destinația finală, cu atât mai multe puncte de eșec potențial și o suprafață mai mare pentru atacuri de securitate. În ciuda acestui fapt, creșterea conectivității cloud prin intermediul internetului public nu a dat niciun semn de încetinire. Internetul public rămâne, de departe, cea mai frecventă modalitate de accesare a cloud-ului (vezi Figura 2.61.).

Avantaje	Dezavantaje
Cel mai bun pentru locații unice	Un serviciu "best-effort" care nu este potrivit pentru aplicații critice
Rentabil pentru volume mici și medii de transfer de date	Rutele partajate și dinamice înseamnă că nu există optimizare a performanței sau performanță garantată
Potrivit pentru majoritatea topologiilor (premise/wan la un singur cloud, premise/wan la multi-cloud)	Nu este potrivit pentru conectivitatea de la cloud la cloud
Folosiți conexiunea de internet existentă, ca de obicei în cadrul afacerii dvs.	Devine costisitor pentru viteze de transfer de date mai mari din cauza facturării per Gigabyte out (ieșire)
Ușor de pus în funcțiune, nu este nevoie de un circuit dedicat	Expus la riscuri de securitate, cum ar fi atacurile DoS și DDoS împotriva routerelor și legăturilor.
Livrare și scalare la cerere, de obicei disponibile	Cea mai puțin sigură opțiune de conectivitate

Figura 2.61. Conectare la cloud folosind internetul public (avantaje și dezavantaje)

Conectivitate cloud utilizând internetul public și prioritizarea cloud-ului

Conectivitatea la internet cu prioritizare cloud vă permite să rezervați în mod dinamic o parte din lățimea de bandă normală a internetului pentru anumite aplicații cloud. Stabilirea priorităților de trafic este eficientă atât pentru traficul de intrare, cât și pentru cel de ieșire, permițând o experiență de utilizare consecventă, susținută de SLA, special pentru traficul dvs. către cloud.

Stabilirea priorităților în cloud este oferită de furnizorii de servicii de rețea care au servicii de peering directe cu furnizorii de cloud, cum ar fi Microsoft. De exemplu, Microsoft Azure Peering Services (pe

scurt, MAPS) permite utilizatorilor finali accesul direct la serviciile de cloud Microsoft prin intermediul furnizorilor de rețea certificați.

Odată implementat, traficul în cloud rămâne complet în rețeaua furnizorului dumneavoastră, ocolind internetul public și evitând orice alt furnizor de servicii de internet intermediar.

Stabilirea priorităților în cloud combină avantajele rutelor optimizate și ale infrastructurii de peering direct cu prioritizarea traficului pe ultima sută de metri, între routerul clientului și limita furnizorului.

Avantaje	Dezavantaje
Un supliment la serviciile standard de acces la Internet	Ofertele depind de furnizorii dvs. de conectivitate și cloud
Performanță consistentă și garantată de SLA până la cel mai apropiat punct de peering	Numai accesul la nivelul 3
Lățime de bandă rezervată în mod dinamic pentru aplicațiile cloud	Fără conexiune dedicată
Funcționează atât pentru lățimea de bandă de intrare, cât și pentru cea de ieșire	
Rutarea optimizată selectează cea mai scurtă cale către marginea rețelei cloud.	
Evită conflictul de rețea și schimbările imprevizibile de rutare	
30 milisecunde Întârziere la deplasare dus-întors (RTD)	
Controlul congestionării traficului *	

**disponibil doar la unii furnizori MAPS*

Figura 2.62. Conectare la cloud folosind internetul public și prioritizarea în cloud (avantaje și dezavantaje)

Conectare directă la cloud prin Eternet

Conectivitatea dedicată prin intermediul serviciilor de conectivitate Ethernet este cea mai rapidă și mai sigură cale pentru conectivitatea în cloud și prima dintre soluțiile de ocolire a internetului. Este rezultatul colaborării furnizorilor de servicii, precum Amazon, Microsoft, Google, Oracle și IBM, cu furnizorii de servicii de rețea pentru a îmbunătăți conectivitatea cloud de la un capăt la altul și capacitățile de automatizare - fără a atinge internetul. Utilizatorii finali sunt probabil deja familiarizați cu numele acestor programe de interconectare directă ale CSP - precum AWS Direct Connect, Microsoft ExpressRoute și Google Cloud Interconnect - care permit conectivitatea securizată de la un capăt la altul prin intermediul unui furnizor de servicii de rețea către locația clientului.

Conectivitatea Ethernet directă la cloud face ca problemele de performanță, de calitate a serviciului și de securitate să devină învechite. Aceasta este asigurată de rampele de conectare la cloud în centrele de date în care este prezent furnizorul de servicii cloud. Aceasta conectează sediile sau instalațiile dvs. prin intermediul unui NSP la furnizorul de cloud printr-o legătură dedicată de nivel 2.

Conectivitatea directă în cloud oferă conectivitatea securizată, de înaltă performanță, de la un capăt la altul, necesară pentru a rula aplicații critice care nu pot fi egalate dacă se utilizează doar internetul. Furnizorii de servicii cloud percep de obicei taxe de transfer de date - care sunt diferite atunci când se conectează la cloud prin conectivitate Ethernet directă față de conectivitatea prin internet, astfel încât conectivitatea directă poate fi deosebit de rentabilă dacă este posibil să transportați cantități mari de date din mediul cloud (cunoscut sub numele de "ieșire") către locația dvs.

Avantaje	Dezavantaje
Suportă toate topologiile (premise to cloud, premise to multi-cloud și cloud to cloud)	Potrivit numai pentru un singur site (nu pentru conectivitate multisite/WAN)
Servicii de lățime de bandă de până la 100Gbps disponibile	Necesită un circuit dedicat
Lățimea de bandă este complet dedicată și garantată de la un capăt la altul	Clientul să se ocupe de peeringul BGP
Livrare la cerere și scalare disponibile în mod obișnuit	În mod implicit, un serviciu de nivel 2, unii NSP oferă un router gestionat (L3).
SLA de conectivitate de la un capăt la altul cu latență și performanță deterministă	
Foarte potrivit și eficient din punct de vedere al costurilor pentru un transfer de date mai mare - datorită prețului mai mic pe Gigabyte (ieșire) în afara facturării față de cel prin Internet.	
Nu este supus atacurilor DDOS, deoarece traficul ocolește Internetul public	

Figura 2.63. Conectare directă în cloud Ethernet (avantaje și dezavantaje)

Conectare în cloud de tip MPLS IP VPN

Integrarea conectivității cloud într-un IP-VPN (cunoscut și sub numele de IP-VPN cloud connect sau tehnologie MPLS-WAN) este o modalitate scalabilă și rentabilă de accesare a serviciilor cloud.

MPLS IP-VPN oferă o lățime de bandă mare, directă și securizată în cloud. conectivitate sigură la furnizorii de servicii cloud. Acesta este potrivit pentru clienții care au nevoie de acces securizat la cloud în mai multe locații și a fost în mod tradițional o modalitate obișnuită de conectare a întreprinderilor la furnizorii de cloud.

Conexiunea cloud este integrată direct în IP VPN, astfel încât este complet privată, fără a depinde de internet. Locațiile cloud sunt integrate în rețeaua WAN privată și sunt considerate efectiv ca un alt site (sau site-uri) în IP-VPN, ceea ce înseamnă că nu este nevoie de reproiectarea rețelelor corporative mari. Diferitele locații ale clienților din IP-VPN împart apoi conectivitatea pentru a-și accesa resursele din cloud.

Avantaje	Dezavantaje
Foarte potrivit pentru integrarea în rețelele IP-VPN MPLS existente și noi	Numai MPLS, fără Internet Sucursale
Extrem de sigur, parte a IP-VPN-ului privat	Conectivitate de nivel 3
Nu este nevoie de reproiectarea rețelelor corporative mari	Este necesară o conexiune dedicată
Complet integrat în IP-VPN (any-to-any), evită necesitatea de a efectua backhaul traficului	Poate crește latența - depinde de locația sucursalelor.
Rentabil, deoarece mai multe locații de pe IP-VPN împart conectivitatea către cloud.	
Suportă diferite topologii: Cloud unic, Multi-Cloud și Cloud-to-Cloud	

Figura 2.64. Conexiunea la cloud de tip MPLS IP VPN (avantaje și dezavantaje)

SD WAN (denumit uneori SDWAN, SD WAN Cloud Access sau SD WAN Multi-Cloud) poate conecta infrastructura WAN definită prin software la mai mulți furnizori de servicii cloud (cum ar fi AWS, Microsoft Azure și Google Cloud) pentru a permite o conectivitate directă, de înaltă performanță și sigură la mai multe cloud-uri. Fiecare filială beneficiază de o conectivitate perfectă de la un capăt la altul la furnizorii dvs. de cloud public.

Pentru o conectivitate directă și eficientă din punct de vedere al costurilor la mai multe medii cloud, SD WAN este probabil soluția optimă.

SD WAN oferă capacități de conectivitate sofisticate și cuprinzătoare, cu funcții care includ prioritizare, optimizare, securitate, analiză, furnizare și implementare automată. Acesta reunește o singură viziune coerentă a rețelei întreprinderii, care leagă între ele site-urile WAN, cloud-ul IaaS/SaaS și conectivitatea sucursalelor, de obicei toate într-un singur portal online. Împreună cu capacitățile la cerere, cum ar fi aprovizionarea site-urilor fără atingere și actualizările de lățime de bandă în timp real, SD WAN este o soluție extrem de puternică.

Înainte de SD WAN, traficul era de obicei redirecționat către un site central sau un hub regional, unde o stivă de hardware fizic oferea funcționalități a căror implementare la site-urile satelit era prohibitivă din punct de vedere al costurilor (cum ar fi securitatea și analiza). SD WAN permite acum ca această funcționalitate să fie implementată în software pe o platformă hardware comună. Aceste stive software cuprind diverse funcții software care pot fi încărcate și implementate în mod dinamic și modular, cu o gamă de funcționalități, printre care se numără

- Rețele și rutare.
- Analize.
- Securitate.
- Optimizarea traficului.
- Acces la distanță.
- Şi multe altele

Prin conectarea site-urilor WAN și a infrastructurii cloud, SD WAN poate oferi securitate, performanță și vizibilitate de la un capăt la altul.

Pornind de la MPLS IP VPN de mai sus, SD WAN oferă conectivitate privată la mai mulți furnizori de cloud într-o singură soluție, combinată cu performanța end-to-end susținută de un SLA, securitate end-to-end și analiză end-to-end.

Avantaje	Dezavantaje
Cel mai bun mod de a gestiona infrastructuri multi-cloud (MPLS și sucursale Internet)	Poate necesita modificări și reproiectări semnificative ale rețelei pentru a valorifica toate beneficiile.
Evită complet necesitatea de a redirecționa traficul de la un site de marcă către un CSP sau un centru de date.	Serviciile mai noi, cum ar fi capacitățile la cerere, pot fi limitate.
Lățimea de bandă este complet dedicată și garantată de la un capăt la altul.	Verificați suportul pentru cerințele specifice ale furnizorului dvs. de cloud (CSP)
Aprovizionare și implementare automată	Verificați suportul și foaia de parcurs pentru caracteristici și funcționalități, cum ar fi optimizarea aplicațiilor, analize, SASE și altele.
Selectarea dinamică a căii - rutare inteligentă și dinamică către cea mai bună cale disponibilă	Poate crește latența - depinde de locația sucursalelor.
Caracteristici suplimentare de securitate, cum ar fi FW/NAT, pentru a sprijini domeniul public CSP	
Vizibilitate și gestionare de la un capăt la altul a întregii rețele a întreprinderii	
Suportă toate topologiile - de la WAN la cloud, de la WAN la multi-cloud și de la cloud la cloud	
Suportă, de asemenea, sucursale care se conectează direct la CSP prin SD-WAN, numai prin Internet	

Figura 2.65. Conexiunea la cloud SD WAN (avantaje și dezavantaje)

Nu există o soluție unică pentru toate întreprinderile care se conectează la cloud. Iată cele zece întrebări și considerații de top pentru a vă asigura că veți rămâne pregătiți pentru viitor cu un nou furnizor:

1. Ce nivel de parteneriat aveți cu principalii furnizori de cloud?
2. Câte puncte de prezență în cloudul public aveți?
3. Câte centre de date sunt conectate în prezent la rețeaua dumneavoastră?
4. Câte birouri sunt conectate în prezent la rețeaua dumneavoastră?
5. Oferiți capacități la cerere prin intermediul unui portal software self-service?
6. Centrul dumneavoastră de date și furnizorul de servicii cloud sunt neutre?
7. Cine deține rețeaua de fibră optică - este privată sau închiriată de la o parte terță?
8. Oferiți conectivitate de la un capăt la altul, inclusiv ultimul kilometru?
9. Oferiți SLA-uri garantate, inclusiv pentru latență, pierdere de pachete și debit?
10. Ce lățimi de bandă sunt acceptate pentru conectivitatea cloud?

2.4.3 Configurarea rețelei cloud

Rețelele sunt implementate pentru a izola datele de lumea exterioară deși acest lucru trece adesea neobservat de către utilizatorul obișnuit . Organizațiile se bazează pe rețea pentru a-și conecta dispozitivele și a-și integra sistemele dincolo de barierele geografice, asigurând în același timp o trecere sigură a informațiilor. Acest ghid rapid vă prezintă elementele de bază ale configurării rețelei cloud.

Rețea virtuală

Rețelele virtuale pot fi considerate ca fiind rețele separate în cadrul unei rețele mai mari. Administratorii pot crea un segment de rețea separat format dintr-o serie de subrețele (sau o singură subrețea) și pot controla traficul care circulă prin rețeaua cloud. În funcție de nevoile afacerii dumneavoastră, puteți implementa rețeaua utilizând tehnologia cloud de la un furnizor de servicii cloud (CSP).

Diferența esențială pentru administratorii și arhitecții de cloud computing atunci când vine vorba de proiectarea soluțiilor de rețea în cloud este gradul de control necesar asupra hardware-ului. Atunci când implementați rețelele cloud cu un CSP, aveți puțin control asupra - și probabil puține cunoștințe despre - designul rețelei CSP-ului. Din cauza acestei limitări, rețelele virtuale sunt adesea alegerea de bază atunci când doriți să oferiți o izolare sigură a rețelei.

În cazul unei soluții cloud, aceste rețele virtuale sunt cunoscute sub numele de VNets sau Virtual Private Clouds (VPC). Acestea acționează ca o reprezentare a unei rețele în cloud, oferindu-vă o rețea cloud. Rețelele virtuale oferă următoarele beneficii:

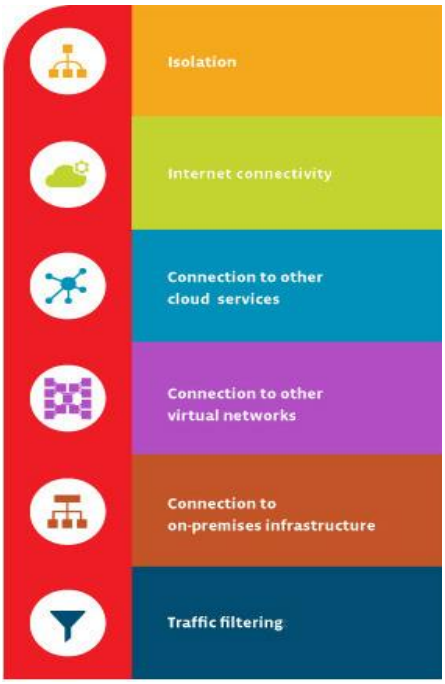

Figura 2.66. Rețele virtuale

- Izolare

Puteți menține rețelele izolate unele de altele pentru a asigura securitatea și în scopul dezvoltării, asigurării calității și implementării rețelelor cloud.

- Conectivitate la internet

Fiecare rețea virtuală poate fi configurată pentru a accesa sau a refuza accesul la internet sau pentru a limita accesul la anumite destinații de pe internet, dacă este necesar.

- Conectarea la alte servicii cloud

Rețelele virtuale au adesea nevoie de o conexiune la serviciile CSP. Acest lucru permite rețelei să utilizeze serviciile oferite de CSP. Furnizorii permit, de obicei, configurarea tabelelor de rutare, a rezoluției numelor de domeniu, a firewall-ului și a elementelor conexe pentru a gestiona conexiunile cu rețelele virtuale.

- Conectarea la alte rețele virtuale

Acest lucru vă permite să vă interconectați rețelele virtuale atunci când este necesar, menținând în același timp controlul asupra conexiunilor.

- Conectarea la infrastructura locală

O parte din flexibilitatea unei rețele virtuale constă în capacitatea de a controla conexiunile. Vă puteți conecta rețeaua virtuală la sistemele locale. Adesea, acest tip de configurație este pentru ca utilizatorii finali să acceseze o rețea cloud privată securizată sau se face ca parte a unei implementări de cloud hibrid.

- Filtrarea traficului

Cele mai multe conexiuni sigure implică filtrarea. În mod normal, aceasta implică filtrarea elementelor în funcție de adresa IP sursă și port, adresa IP destinație și port, precum și de un anumit protocol. Acest lucru le oferă inginerilor de cloud computing un control sporit asupra comunicațiilor care au loc în rețeaua dumneavoastră.

Elemente constitutive ale rețelei cloud

În calitate de administrator cloud sau inginer de cloud computing, capacitatea dvs. de a crea o rețea virtuală se va baza, de obicei, pe un software de mașină virtuală sau pe o rețea cloud furnizată de un CSP. Software-ul de mașină virtuală permite administratorilor de cloud să desemneze și să conFiguraze parametrii rețelei virtuale asociate cu placa de interfață de rețea (NIC) fizică a unei gazde. Atunci când configurați mai multe gazde pentru a funcționa folosind aceiași parametri, adăugați gazdele respective la rețeaua virtuală. Rețelele virtuale trebuie să aibă următoarele componente:

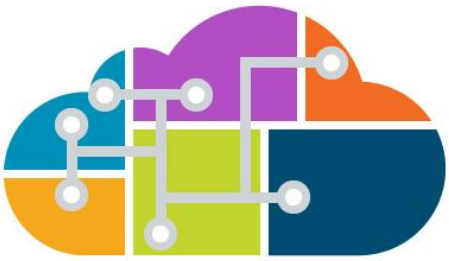

Figura 2.67. Blocurile constructive ale rețelei cloud

- **Comutator virtual**

Comutatoarele virtuale vă oferă posibilitatea de a de a crea segmente în rețeaua dumneavoastră și să conectați aceste componente între ele. Puteți conecta una sau mai multe mașini virtuale la un comutator virtual.

- **Punte virtuală**

Această componentă vă permite să conectați mașinile virtuale la LAN utilizată de computerul gazdă. Puntea virtuală conectează adaptorul de rețea de pe mașina virtuală la NIC-ul fizic de pe computerul gazdă. Se pot configura mai multe punți virtuale pentru a se conecta la mai multe NIC-uri fizice.

- **Adaptor gazdă virtuală**

Adaptorul permite mașinilor virtuale să comunice cu gazda. Adaptoarele de gazdă virtuală sunt comune în cazul mașinilor virtuale numai gazdă și Traducere a adreselor de rețea (NAT) configurații de tip NAT (NAT). Acestea nu se pot conecta la o rețea externă fără un server proxy.

- **Serviciul NAT**

Serviciile NAT permit conectarea la internet a mai multor dispozitive din rețeaua dvs. cloud.

- **Server DHCP**

Serverul DHCP alocă adrese IP mașinilor virtuale și gazdelor. Acest lucru se aplică în cazul configurațiilor doar pentru gazdă și NAT.

- **Adaptor Ethernet**Acesta este un adaptor de rețea fizic instalat pe gazdele care se conectează la rețea.

Mulți CSP oferă servicii de cloud care facilitează configurarea rețelelor virtuale și a rețelelor cloud. În cazul rețelelor cloud, configurați rețeaua virtuală și adăugați resursele la aceasta, în loc să le configurați la nivelul mașinii virtuale. De asemenea, rețelele cloud oferă, de obicei, capacități de simplificare a monitorizării, gestionării, conexiunilor și securității.

Opțiuni de configurare a topografiei rețelei

Dacă doreşti sa faci utilizabilă o reţea virtuală trebuie să conFigurazi şi următoarele componente:

Figura 2.68. Opțiuni de configurare a topografiei rețelei

- **Subrețele**
  Sub-rețelele sunt o parte obligatorie a unei rețele virtuale. Aveți nevoie de subrețele TCP/IP, care vor desemna adresele care sunt utilizate în rețeaua respectivă. Se folosesc adesea intervale de adrese publice și private. Atunci când acest lucru nu este posibil, adresele sunt adesea atribuite de către CSP. Rețelele virtuale pot fi segmentate în una sau mai multe subrețele.
- **Rutere sau tabele de rutare**
  Pentru orice rețea, trebuie să configurați routere sau tabele de rutare pe orice mașină virtuală conectată la rețea, astfel încât pachetele să poată fi rutate în mod corespunzător.
- **DNS**
  Trebuie să furnizați adresele serverului DNS, atribuite fie de dumneavoastră, fie de CSP.
- **Regiunea sau zonele CSP**
  Trebuie specificate rețelele virtuale care funcționează în regiuni CSP diferite. Acest lucru vă va permite, de asemenea, să conectați rețele virtuale din regiuni diferite. Dacă este necesar, puteți configura, de asemenea, izolarea între regiuni.
- **Filtre de traffic**

Configurarea filtrelor de trafic în funcție de specificațiile protocoalelor de securitate va permite doar ca traficul aprobat să treacă prin rețeaua dumneavoastră. Filtrele pot fi aplicate la NIC în mașinile virtuale, la o subrețea sau la un serviciu cloud. Atunci când este necesar, veți face acest lucru cu un dispozitiv virtual de rețea.

Sfaturi pentru proiectarea rețelei cloud

Atunci când proiectați rețelele cloud, luați în considerare următoarele:

- Pe măsură ce vă proiectați rețeaua cloud, faceți-vă timp pentru a compara serviciile de rețea virtuală oferite de furnizorii de cloud. O rețea cloud găzduită poate fi singura modalitate prin care puteți crea rețele virtuale așa cum doriți. Adesea, aceste rețele cloud sunt mai ușor de configurat și de gestionat.
- Dacă intenționați să filtrați traficul (și majoritatea companiilor ar trebui să o facă!), planificați testarea filtrului în cadrul implementării pentru a evita viitoarele plângeri ale utilizatorilor din cauza traficului blocat.
- Dacă alegeți să apelați la un CSP, colaborați cu personalul acestuia pentru a configura componentele rețelei cloud, cum ar fi tabelele de rutare, dispozitivele virtuale de rețea și subrețele. Scăpați de unele probleme de la început.

Porturile și protocolul rețelei cloud

Unul dintre pașii cheie pe care trebuie să îi faceți pentru a vă securiza rețeaua de cloud computing este să intrați în detalii pentru a descoperi ce persoane, servicii și tehnologii au nevoie de acces la rețea. Porturile sunt o parte esențială a rețelei dvs. cloud. Portul este punctul final al conexiunii dumneavoastră.

Utilizatorii se conectează la rețeaua de cloud prin intermediul unui port de desemnare. Tuturor porturilor li se atribuie un număr cuprins între 0 și 65.535. Internet Assigned Numbers Authority (IANA) separă numerele de port în trei porturi, în funcție de numărul acestora. Porturile TCP și UDP sunt atribuite pe baza acestor intervale. Hackerii urmăresc în mod obișnuit porturile bine cunoscute, dar se știe că vizează și porturile deschise înregistrate sau dinamice.

Cele trei porturi sunt:

- Porturi bine-cunoscute
  Preatribuite proceselor de sistem de către IANA, acestea includ de la 0 la 1.023 și sunt cele mai predispuse la atacuri.
- Porturi înregistrate
  Disponibile pentru procesele utilizatorilor și listate de IANA, aceste porturi înregistrate merg de la 1.024 la 49.151 și sunt cunoscute ca fiind prea specifice sistemului pentru a fi ținta directă a

hackerilor. Cu toate acestea, hackerii caută uneori porturi deschise în acest interval. Nu le întoarceți spatele, dar puteți să vă abateți privirea ocazional.

- Porturi dinamice sau private

  Atribuite de un sistem de operare client în funcție de necesități, acestea sunt porturile numerotate de la 49.152 la 65.535. Porturile dinamice se schimbă în mod constant (de aici și denumirea de dinamice), astfel încât este dificil să se țintească direct numerele. Dar, din nou, se știe că hackerii au scanat porturile deschise. În ceea ce privește urmărirea hackerilor, poate că puteți întoarce spatele porturilor dinamice sau private, dar nu pentru prea mult timp!

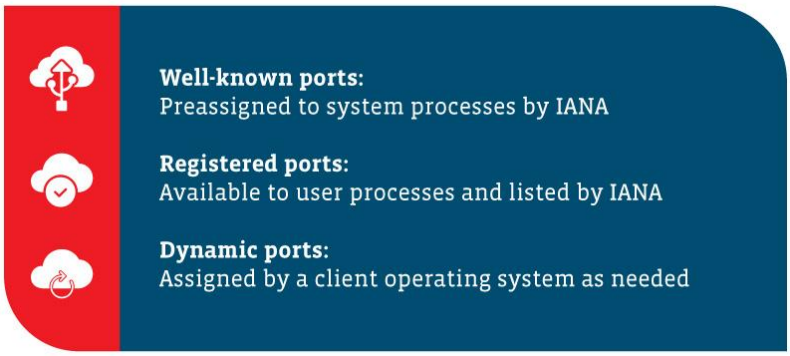

Figura 2.69. Porturi dinamice sau private

Deci, la ce sunt folosite aceste porturi? Iată o listă a unora dintre cele mai comune porturi de rețea implicite utilizate în lumea tehnologiei:

- 21 FTP (File Transfer Protocol)
- 22 SSH (Secure Shell)
- 25 SMTP (Simple Mail Transfer Protocol)
- 53 DNS (Domain Name System)
- 80 HTTP (Hypertext Transfer Protocol)
- 110 POP3 (Protocolul oficiului poștal)
- 139 Serviciul de sesiuni NetBIOS
- 143 IMAP (Internet Message Access Protocol)
- 443 HTTPS (Hypertext Transfer Protocol Secure)
- 3389 RDP (Remote Desktop Protocol)

Întreținerea rețelei dvs. Cloud

Serviciile și aplicațiile care plutesc în cloud sunt similare în multe privințe cu serviciile și aplicațiile care rămân ancorate în infrastructura dvs. locală. Luați, de exemplu, aplicațiile web și serviciile de directoare bazate pe cloud. Multe dintre ele vor folosi aceleași porturi și protocoale care sunt folosite de omologii

lor locali. Instrumentele de gestionare, fie că sunt bazate pe CSP, fie că sunt terțe sau cele construite de echipa dvs. IT, vor utiliza, de asemenea, cerințele privind porturile și protocoalele.

Dacă vă decideți să faceți saltul de la pământ (locaţia proprie) la nor (cloud), va trebui să vă revizuiți porturile pentru a determina ce trebuie să se bazeze pe cloud și ce trebuie să rămână în infrastructura proprie. Analizați cu atenție ce (aplicaţie) are nevoie de acces la internet, pentru a comunica cu servicii sau aplicații externe, și ce tip de acces este necesar din interiorul cloud-ului.

Odată ce ați restrâns aria de acoperire, puteți configura firewall-uri și puteți seta filtrele necesare pentru a vă asigura că rețeaua dvs. cloud va rămâne sigură. Pe măsură ce lucrați la implementarea rețelei cloud, asigurați-vă că veţi consulta următoarele resurse:

Figura 2.70. Întreținerea rețelei dvs. de cloud

- Ghidurile de configurare a aplicațiilor și serviciilor pentru a identifica porturile și protocoalele necesare pe care le utilizează fiecare dintre ele.
- Ghidurile de securitate și de implementare a CSP sau cărțile albe pentru a localiza porturile și protocoalele de care aveți nevoie pentru a accesa serviciile cloud, cum ar fi site-urile web, bazele de date, serviciile de directoare și așa mai departe.
- Ghiduri de implementare de la terți care sunt similare cu rețeaua cloud pe care o implementați.
- Propria documentație (da, propria documentație) pentru a face referire la firewall, rutare și alte informații conexe care vă pot ajuta să înțelegeți utilizarea porturilor și a protocoalelor. Va fi dificil să implementați cu succes un sistem de implementare în cloud dacă nu aveți nicio idee de unde săriți.
- Dacă sorții vă interzic să descoperiți ce porturi și protocoale sunt folosite de o aplicație veche pe care doriți să o mutați în cloud, ar fi bine să adunați câteva instrumente utile, cum ar fi un scaner de porturi sau un analizor de protocoale, pentru a dezvălui secretele păzite de predecesori.

Înainte de a lansa orice rețea cloud, verificați cu atenție toate aplicațiile și serviciile pentru a vă asigura că toate porturile și protocoalele sunt conforme.

Determinarea acordării accesului la rețeaua cloud

Înainte de a da acele permise de intrare magice și de a acorda acces la rețeaua cloud, luați în considerare aceste orientări, pe lângă informațiile deja furnizate:

- Nu presupuneți că știți toate porturile legate de un serviciu de aplicație. Știți ce înseamnă să presupui, nu? Nu vă aflați la capătul ei.
- Acordați o atenție deosebită direcției fluxului de trafic atunci când creați reguli de intrare și de ieșire pentru accesul la rețea.

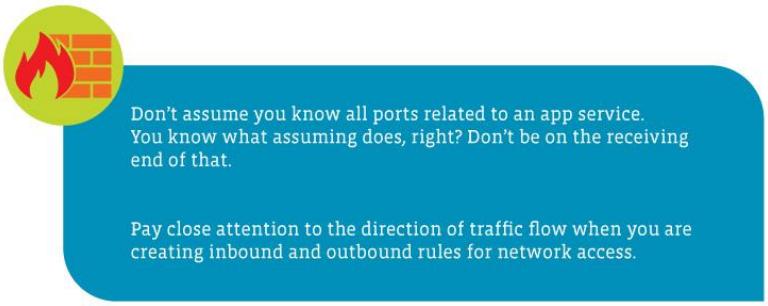

Figura 2.71. Determinarea acordării accesului la rețeaua cloud

2.5 Managementul(Gestionarea) sistemului cloud (Serviciul de Monitorizare și Notificare)

Nivel de dificultate: Uşor
Perioada de finalizare:
Obiective:
După ce va citi acest material, cititorul va înțelege conceptul de Cloud Management, sistemele de Cloud Management și instrumentele de monitorizare. De asemenea, va cunoaște principalele obiective și caracteristici ale Cloud Management, platforme, instrumente și furnizori.

Figura 2.72. Managementul sistemului cloud

Realizări:

După ce veți completa această aplicație, veți putea:

- să știți la ce se referă managementul cloud;
- cum funcționează managementul cloud;
- importanța managementului cloud;
- obiectivele și caracteristicile managementului cloud;
- cele 4 tipuri de gestionare a cloud-ului;
- cunoaste la ce se referă Could Monitoring;
- provocările monitorizării Cloud.
- analiza platformelor, instrumentelor și furnizorilor de gestionare a cloud-ului

Introducere în managementul cloud-ului și în sistemele de management al cloud-ului

Ce este Managementul Cloud-ului?

Gestionarea cloud-ului se referă la exercitarea controlului asupra resurselor și serviciilor de infrastructură cloud publice, private sau hibride. O strategie de gestionare a cloud-ului bine concepută poate ajuta experții IT să controleze mediile de calcul dinamice și scalabile.

Managementul cloud-ului este **procesul de monitorizare și de maximizare a eficienței în utilizarea unuia sau mai multor cloud-uri private sau publice.** Organizațiile folosesc de obicei o platformă de gestionare a cloud-ului pentru a gestiona utilizarea cloud-ului. Mai mult, managementul cloud-ului este **o metodă de revizuire, observare și gestionare a fluxului de lucru operațional într-o infrastructură IT bazată pe cloud**. Tehnicile de gestionare manuală sau automată confirmă disponibilitatea și performanța site-urilor web, a serverelor, a aplicațiilor și a altor infrastructuri cloud.

De ce se folosește managementul cloud?

Organizațiile implementează din ce în ce mai multe aplicații de întreprindere în cloud pentru a reduce investițiile inițiale ridicate pe care ar trebui să le facă pentru infrastructura la fața locului. Mediile cloud publice oferă putere de calcul și stocare de date la cerere, în concordanță cu cererea tot mai mare și fluctuantă de date și servicii. Prin intermediul gestionării serviciilor cloud, administratorii supraveghează activitățile cloud, de la implementarea și utilizarea resurselor, la gestionarea ciclului de viață al resurselor, integrarea datelor și recuperarea în caz de dezastru.

Cum funcționează managementul cloud?

Rezumând toate cele de mai sus, managementul cloud este o disciplină care este facilitată de instrumente și software. Pentru a realiza controlul și vizibilitatea necesare pentru o gestionare eficientă a cloud-ului, întreprinderile sau orice altă parte interesată ar trebui să își vadă infrastructura IT hibridă

prin intermediul unei platforme consolidate care să extragă datele relevante din toate sistemele organizației bazate pe cloud și din sistemele tradiționale de la fața locului.

Platformele de gestionare a cloud-ului ajută echipele IT să securizeze și să optimizeze infrastructura cloud, inclusiv toate aplicațiile și datele care se află pe aceasta. Administratorii pot gestiona conformitatea, pot configura o monitorizare în timp real și pot anticipa atacurile cibernetice și încălcările de date.

Deci, cum funcționează? În mod obișnuit, un sistem de gestionare a cloud-ului este instalat pe un cloud vizat menționat. După capturarea informațiilor privind activitatea și performanța, se trimite o analiză către un tablou de bord bazat pe web. Acolo, administratorii pot observa și reacționa în consecință. În cazul în care apare vreo problemă, administratorii pot transmite comentarii către cloud prin intermediul platformei de gestionare a cloud-ului.

Importanța managementului cloud-ului

Este mai probabil ca întreprinderile/organizațiile să îmbunătățească performanța, fiabilitatea, limitarea costurilor și durabilitatea mediului în cloud computing. Gestionarea aplicațiilor conține sarcini repetitive care, prin intermediul serverelor de gestionare în cloud și al codului push, pot fi furnizate automat prin intermediul API-urilor, în locul gestionării manuale.
Managementul cloud poate juca un rol important în gestionarea stării de securitate și a vulnerabilității activelor IT.

Obiectivele și caracteristicile managementului cloud

Fără îndoială, cea mai mare provocare pentru gestionarea cloud-ului este extinderea cloud-ului[1] - personalul IT pierde urma resurselor cloud, care se înmulțesc apoi necontrolat în întreaga organizație. Extinderea în cloud poate crește costurile și poate crea probleme de securitate și de gestionare, astfel încât magazinele IT au nevoie de politici de guvernanță și de controale de acces bazate pe roluri.

Essential areas of cloud management include the automated and orchestrated instances and configurations, secure access and policy adherence, and monitoring at all levels -- all done as cost-efficiently as possible.

Figura 2.73. Componentele gestionarii cloudului

Platformele de gestionare a cloud-ului oferă o perspectivă comună asupra tuturor resurselor cloud pentru a ajuta la monitorizarea serviciilor cloud interne și externe. Instrumentele platformei de gestionare pot ajuta la ghidarea tuturor persoanelor care vin in contact cu aplicatiile in ciclul lor de viață. Auditurile regulate pot menține resursele sub control. În cele din urmă, luați în considerare instrumente de la terți pentru a ajuta la reglarea fină a utilizării, performanței, costurilor și beneficiilor de afaceri ale întreprinderii.

Este necesar să se stabilească parametrii pentru a ajuta la identificarea tendințelor și pentru a oferi orientări cu privire la ceea ce utilizatorul dorește să măsoare și să urmărească în timp. Există o mulțime de puncte de date potențiale, dar fiecare întreprindere/parte interesată ar trebui să le aleagă pe cele care contează cel mai mult pentru afacerea/organizația/proiectul lor.

Din punct de vedere mai analitic, trebuie să se ia în considerare următoarele aspecte:

- Datele privind utilizarea volumului și a performanței unei instanțe de calcul (procesor, memorie, disc etc.) oferă informații despre starea generală a aplicației;
- Consumul de spațiu de stocare se referă la spațiul de stocare legat de instanțele de calcul;
- Serviciile de echilibrare a încărcării distribuie traficul de intrare în rețea;
- Instanțele de baze de date ajută la colectarea și analiza datelor;

- Instanțele de memorie cache utilizează memoria pentru a păstra datele accesate frecvent și, astfel, evită necesitatea de a utiliza medii mai lente, cum ar fi stocarea pe disc;
- Funcțiile, denumite și servicii de calcul fără server, sunt utilizate pentru a furniza sarcini de lucru și pentru a evita necesitatea de a furniza și de a plăti pentru instanțe de calcul. Furnizorul de cloud operează serviciul care încarcă, execută și descarcă funcția atunci când aceasta îndeplinește parametrii de declanșare.

Tipuri de management a cloud-ului

Există patru (4) tipuri principale de calcul, care sunt clasificate în cloud-uri **private, cloud-uri publice, cloud-uri hibride și multi-clouds.**

Mai analitic:

- **Cloud-uri private: sunt** definite ca fiind servicii informatice oferite fie prin internet, fie printr-o rețea internă privată și numai unor utilizatori selectați, în locul publicului larg. Denumit și cloud intern sau corporativ, cloud computing-ul privat oferă întreprinderilor/organizațiilor multe dintre avantajele unui cloud public - inclusiv autoservirea, scalabilitatea și elasticitatea - cu controlul și personalizarea suplimentare disponibile prin resurse dedicate pe o infrastructură de calcul găzduită la fața locului. Cloud-urile private oferă un nivel mai ridicat de securitate și confidențialitate atât prin firewall-urile companiei, cât și prin găzduirea internă, pentru a se asigura că operațiunile și datele sensibile nu sunt accesibile furnizorilor terți.
- **Cloud-uri publice:** Modele IT prin care furnizorii de servicii de cloud public pun la dispoziția organizațiilor și persoanelor fizice, la cerere, servicii de calcul - inclusiv calcul și stocare, medii de dezvoltare și implementare și aplicații - prin intermediul internetului public.
- **Cloud-uri hibride:** numit uneori cloud hibrid - este un mediu de calcul care combină un centru de date local (numit și cloud privat) cu un cloud public, permițând partajarea datelor și aplicațiilor între acestea.
- **Multi-cloud-uri**: utilizarea de către o companie/organizație a mai multor servicii de cloud computing și de stocare de la diferiți furnizori într-o singură arhitectură eterogenă pentru a îmbunătăți capacitățile și costurile infrastructurii cloud. Se referă, de asemenea, la distribuirea activelor, a software-ului, a aplicațiilor etc. în cloud în mai multe medii de găzduire în cloud.

Instrumente de management și monitorizare a cloud-ului

Monitorizarea cloud este **o metodă de revizuire, observare și gestionare a fluxului de lucru operațional într-o infrastructură IT bazată pe cloud**. Tehnicile de gestionare manuală sau automată confirmă disponibilitatea și performanța site-urilor web, a serverelor, a aplicațiilor și a altor infrastructuri cloud. Monitorizarea cloud-ului măsoară condițiile unui volum de lucru și diverși parametri cuantificabili care se referă la operațiunile globale de cloud. Rezultatele sunt monitorizate în date specifice, granulare, dar aceste date sunt adesea lipsite de context.

Observabilitatea cloud-urilor este un proces similar monitorizării cloud-ului, în sensul că ajută la evaluarea sănătății cloud-ului. Observabilitatea se referă mai puțin la măsurători, ci mai degrabă la ceea ce se poate desprinde dintr-un volum de lucru pe baza proprietăților sale vizibile din exterior. Există două aspecte ale observabilității cloud-ului: metodologia și starea de funcționare. Metodologia se concentrează pe aspecte specifice, cum ar fi metricele, urmărirea și analiza jurnalelor. Starea de operare se bazează pe urmărire și abordează identificarea stării și relațiile dintre evenimente, acestea din urmă făcând parte din DevOps.

Provocările monitorizării cloud

Una dintre cele mai mari provocări ale monitorizării Cloud pentru echipele IT este aceea de a ține pasul cu proiectele de aplicații moderne și distribuite. Pe măsură ce aplicațiile evoluează, echipele IT trebuie să își adapteze mereu strategiile de monitorizare.

Monitorizarea eficientă a cloud-ului este o sarcină complexă. Este posibil ca instrumentele pe care o organizație le utilizează în prezent să nu mai fie cele de care are nevoie, deoarece diferite tipuri de aplicații vor trebui monitorizate în moduri diferite.

De ce depinde succesul ?

Succesul oricărei strategii de gestionare a cloud-ului depinde nu doar de utilizarea adecvată a instrumentelor și a automatizării, ci și de existența unui personal IT competent. Echipele IT și cele de afaceri trebuie să colaboreze în mod natural pentru a asimila o cultură cloud și a înțelege obiectivele afacerii/organizației.

Echipele IT trebuie, de asemenea, să testeze performanța aplicațiilor cloud, să monitorizeze parametrii de cloud computing, să ia decizii critice în materie de infrastructură, să rezolve problema patch-urilor și a vulnerabilităților de securitate și să actualizeze regulile de afaceri care conduc managementul cloud. Întreprinderile/organizațiile care nu dispun de personal calificat în domeniul IT pot solicita întotdeauna asistență din partea unor terți. Aplicațiile terților susțin alertele privind pragul bugetar care pot notifica finanțele și părțile interesate din linia de afaceri, astfel încât acestea să poată monitoriza cheltuielile pentru cloud. Brokerii de cloud dispun adesea de un catalog de servicii și de unele instrumente de gestionare financiară. Momentul de a examina cu atenție cheltuielile pentru cloud este la început, atunci când aplicațiile intră în producție.

Platforme, instrumente și furnizori pentru managementul cloud-ului

Pe măsură ce cloud computing-ul se extinde în întreaga întreprindere, o platformă generală de gestionare a cloud-ului poate ajuta la implementarea, gestionarea și monitorizarea tuturor resurselor cloud. Întreprinderea IT trebuie să își formeze o idee clară cu privire la ceea ce dorește să monitorizeze înainte de a a evalua platformele de gestionare a cloud-ului care să se potrivească acestor nevoi - fie că

este vorba de instrumente individuale care rezolvă o singură problemă, cum ar fi performanța rețelei sau analiza traficului, fie de o suită cuprinzătoare care analizează totul. Unele dintre aceste decizii vor cântări instrumente de la furnizorii de cloud, cum ar fi instrumente de securitate de la furnizorii de platforme cloud sau de la furnizori terți.

Cel mai cuprinzător produse de management a cloud-ului oferă caracteristici care acoperă aceste cinci categorii:

- automatizare și orchestrare pentru aplicații și mașini virtuale individuale;
- securitate, inclusiv gestionarea identității și protecția și criptarea datelor;
- guvernanța și conformitatea politicilor, inclusiv auditurile și acordurile privind nivelul serviciilor;
- monitorizarea performanțelor;
- gestionarea costurilor.

Numeroși furnizori de gestionare multi-cloud oferă o gamă de instrumente, fiecare cu puncte forte și puncte slabe.
Unele dintre cele mai importante sunt VMware (un furnizor de software de virtualizare și cloud computing cu sediul în Palo Alto, California. Fondată în 1998, VMware este o subsidiară a Dell Technologies) CloudBolt Software, (o platformă de management cloud hibrid dezvoltată de CloudBolt Software pentru implementarea și gestionarea mașinilor virtuale (VM), aplicațiilor și a altor resurse IT, atât în cloud-uri publice (de exemplu, AWS, MS Azure, GCP), cât și în centre de date private (de exemplu, VMware, OpenStack)), Snow Software (care a achiziționat Embotics, este un dezvoltator de testare a pieței de instrumente de gestionare a activelor software), Morpheus Data (o noua abordare in furnizarea accesului de la distanta a datelor micro ale statisticilor oficiale), Scalr (un furnizor de tehnologie a informației (IT) care oferă o platformă de management pentru cloud computing) și Flexera (este specializată în software de management IT, optimizare și soluții). De asemenea, în acest mix se află și furnizorii tradiționali de gestionare a serviciilor IT, cum ar fi BMC Software ((BMC)- baseboard management controller, este un procesor de servicii specializat care monitorizează starea fizică a unui computer, server de rețea sau alt dispozitiv hardware folosind senzori și comunicând cu administratorul de sistem printr-o conexiune independentă), CA Technologies (una dintre cele mai mari companii independente de software din lume; compania, care a fost cunoscută anterior ca Computer Associates International, este o corporație multinațională americană publică), Micro Focus (o afacere multinațională britanică de software și tehnologia informației) și ServiceNow (o platformă de automatizare a fluxului de lucru bazată pe cloud, care permite organizațiilor întreprinzătoare să îmbunătățească eficiența operațională prin eficientizarea și automatizarea sarcinilor de lucru de rutină), care deservesc de obicei marile companii cu procese de guvernanță ITSM (ITSM: IT Service Management Software).

Companiile IT care utilizează un singur cloud public ar putea dori să se limiteze la instrumentele oferite de furnizorul de servicii respectiv, deoarece aceste instrumente sunt concepute pentru a îmbunătăți platformele de gestionare native. În ceea ce privește monitorizarea cloud, Google Cloud Operations (fostul Stackdriver) monitorizează Google Cloud, precum și aplicațiile și VM-urile care rulează pe AWS Elastic Compute Cloud. Microsoft Azure Monitor colectează și analizează datele și resursele din cloud-ul Azure. Există, de asemenea, multe opțiuni open source de monitorizare a cloud-ului pentru întreprinderile care se simt confortabil să lucreze cu instrumente open source.

3 APLICAŢII

3.1 Acces la o bază de date folosind amprenta unei persoane ca parolă

Scop

Bazele de date conțin uneori date foarte importante pentru unele companii sau organizații. Accesarea acestor date este permisă pentru un număr mic de persoane. Pentru a crește nivelul de securitate, accesul la aceste date trebuie să se bazeze pe indici specifici pentru persoanele care au drept de acces. Aplicația permite accesul la baza de date pe baza amprentei persoanelor care au dreptul de a accesa baza de date.

Perioada de timp estimată pentru a obţine avantaje

3 săptămâni – 2 luni

3.2 Server Active Directory

Scop

Scopul unui server Active Directory (AD) este de a oferi o locație centralizată pentru gestionarea resurselor de rețea, cum ar fi conturile de utilizator, computerele și imprimantele. Este un depozit de baze de date care stochează informații despre toți utilizatorii și dispozitivele conectate la o rețea și permite utilizatorilor autorizați să acceseze resursele din rețea. Serverul AD acționează ca un serviciu director și este responsabil pentru gestionarea procesului de autentificare și autorizare pentru utilizatorii care încearcă să acceseze resursele rețelei. Acest lucru le permite administratorilor de sistem să impună politici de securitate în întreaga organizație, asigurându-se că numai utilizatorii autorizați pot accesa anumite resurse. Serverul AD permite, de asemenea, delegarea sarcinilor administrative către diferite persoane sau grupuri, ceea ce poate îmbunătăți gestionarea și eficiența în cadrul unei organizații. În general, obiectivul principal al unui server AD este de a simplifica administrarea rețelei,

de a îmbunătăți securitatea și de a oferi o locație de gestionare centralizată pentru toate resursele rețelei.

Perioada de timp estimată pentru a obține avantaje

Perioada de timp estimată pentru a crea aplicatia cu un server Active Directory (AD) depinde de nevoile și cerințele specifice ale organizației. Cu toate acestea, unele beneficii pot fi sesizate imediat după implementare, în timp ce sesizarea altora poate dura mai mult.

În ceea ce privește beneficiile imediate, un server AD poate simplifica administrarea rețelei prin centralizarea managementului utilizatorilor. Acest lucru poate îmbunătăți eficiența și poate reduce timpul și efortul necesar pentru sarcinile IT obișnuite, cum ar fi resetarea parolelor sau crearea de noi conturi de utilizator. În plus, AD poate îmbunătăți foarte mult securitatea rețelei prin furnizarea unei locații centralizate pentru impunerea politicilor de securitate și gestionarea accesului la resursele rețelei. Acest lucru poate ajuta la reducerea riscului de încălcări de securitate și acces neautorizat la datele companiei.

Alte beneficii, cum ar fi îmbunătățirea scalabilității și flexibilității, pot dura mai mult timp pentru a se realiza. De exemplu, infrastructura AD poate sprijini creșterea organizației în timp, oferind o bază scalabilă și fiabilă pentru gestionarea și autentificarea utilizatorilor. Acest lucru poate ajuta la reducerea costurilor și la creșterea eficienței pe măsură ce organizația se extinde.

Per total, intervalul de timp estimat pentru a crea valoare cu un server AD depinde de diverși factori, cum ar fi dimensiunea și complexitatea organizației și cerințele tehnice specifice ale implementării. Unele beneficii pot fi realizate imediat, în timp ce altele pot dura mai mult. Cu toate acestea, un server AD poate fi o investiție valoroasă în ceea ce privește reducerea cheltuielilor administrative, creșterea securității și furnizarea unei infrastructuri scalabile pentru creșterea pe termen lung a organizației.

3.3 Sisteme de analiză a comportamentului AI

Scop

Scopul sistemelor de analiză a comportamentului AI este de a analiza și interpreta modelele de comportament uman și de a prezice comportamentul viitor pe baza unor perspective bazate pe date. Acesta urmărește să ofere o înțelegere mai profundă a comportamentului uman și a procesului de luare a deciziilor și să identifice potențiale riscuri, amenințări sau oportunități în diferite domenii, cum ar fi poliția, sănătatea, securitatea și marketingul. Prin folosirea algoritmilor de învățare automată și a tehnicilor de extragere a datelor, aceste sisteme urmăresc să identifice modele și anomalii de comportament care ar putea indica potențiale amenințări sau probleme. Scopul final este de a valorifica informațiile din analiza comportamentului pentru a îmbunătăți procesul decizional, a reduce riscurile și a îmbunătăți rezultatele în numeroase domenii.

Perioada de timp estimată pentru a obține avantaje

Perioada de timp pentru a crea valoare din sistemele de analiză a comportamentului AI depinde de mai mulți factori, cum ar fi complexitatea problemei care umează să fie rezolvată, calitatea și accesibilitatea datelor și tehnologia utilizată.

În scenarii mai simple, valoarea poate fi creată relativ rapid, cum ar fi în câteva luni. De exemplu, dacă o companie folosește sisteme de analiză a comportamentului pentru a-și optimiza strategiile de marketing, poate vedea rezultate în doar câteva luni. Pe de altă parte, scenariile mai complexe, cum ar fi utilizarea sistemelor de analiză a comportamentului pentru a detecta frauda sau a preveni încălcările de securitate, pot necesita un interval de timp de asteptare pentru a crea valoare și poate dura câțiva ani pentru a se realiza pe deplin.

În general, un sistem de analiză a comportamentului AI bine implementat poate aduce beneficii imediate ale îmbunătățirii procesului de luare a deciziilor și ale diminuării riscurilor, dar întregul potențial al unor astfel de sisteme poate dura mai mult până se materializează. Pe măsură ce algoritmii devin mai avansați și seturile de date devin mai cuprinzătoare, valoarea creată de aceste sisteme va continua probabil să crească în timp.

3.4 Aplicație pentru de gestionare a activității de închiriere de scule și echipamente de la o firmă către persoane fizice

Scop

În multe situații, persoanele care desfășoară activități de reparații la propriile locuințe au nevoie de instrumente specifice pentru aceste activități. Unele activități de reparații sau construcții se desfășoară rar și nu este justificată achiziționarea de unelte sau echipamente necesare pentru activitatea respectivă.

O solutie este inchirierea acestui echipament de la firme care au acest obiect de activitate. Aplicația gestionează activitatea de închiriere de scule și echipamente ale unei companii către persoane sau alte companii care utilizează acest echipament.

Perioada de timp estimată pentru a obține avantaje

1 săptămână-1 lună

3.5 Aplicație pentru monitorizarea echipamentelor autonome de curățare a încăperii (aspiratoare) la sediile întreprinderilor mici și mijlocii sau în locuințe particulare

Scop

Aplicaţia permite monitorizarea activităţii unui aspirator sau mai multor aspiratoare care funcţionează autonom într-un spațiu inchis. Aspiratoarele sunt folosite pentru curăţarea camerelor de zi sau a birourilor.

Aspiratoarele care pot fi acţionate prin telecomandă și care se pot deplasa autonom fără a fi purtate de o persoană, fac curăţenia unei camere mai uşoară.

Aceste aspiratoare sunt echipate cu diferite tipuri de senzori care detectează apropierea unui obstacol și schimbă direcția de mișcare a aspiratorului. Direcția de mișcare a aspiratorului depinde de modul în care a fost scris algoritmul de funcționare al aspiratorului de către producător.

Aplicaţia creează un algoritm de deplasare a aspiratorului în spațiul încăperii astfel încât operaţia de curăţare să fie eficientă.

Perioada de timp estimată pentru a obţine avantaje

4 săptămâni-3 luni

3.6 Urmărirea activelor

Scop

Scopul urmăririi activelor este de a monitoriza și gestiona locația fizică și starea activelor, cum ar fi echipamentele, materialele și produsele, pe măsură ce acestea se deplasează prin lanțul de aprovizionare. Sistemele de urmărire a activelor utilizează tehnologii avansate, cum ar fi identificarea cu frecvență radio (RFID), sistemul de poziționare globală (GPS) și codurile de bare pentru a oferi informații în timp real despre locația, starea și mișcările activelor.

Unele dintre obiectivele cheie ale urmăririi activelor includ:

- Vizibilitate: sistemele de urmărire a activelor oferă vizibilitate asupra locației și stării activelor, permițând organizațiilor să știe în orice moment unde sunt activele lor.
- Conformitate: sistemele de urmărire a activelor ajută organizațiile să respecte reglementările, oferind date fiabile despre mișcarea și manipularea activelor reglementate, cum ar fi produsele farmaceutice și materialele periculoase.

- Eficiență: sistemele de urmărire a activelor minimizează necesitatea verificărilor manuale ale inventarului și îmbunătățesc eficiența lanțului de aprovizionare prin furnizarea de informații în timp real despre mișcările activelor.
- Reducerea costurilor: sistemele de urmărire a activelor pot reduce costurile asociate cu activele pierdute, furate sau deplasate și pot reduce timpul și forța de muncă necesare pentru gestionarea stocurilor.
- Procesul decizional îmbunătățit: sistemele de urmărire a activelor furnizează date care pot fi utilizate pentru a sprijini o mai bună luare a deciziilor, cum ar fi optimizarea operațiunilor lanțului de aprovizionare, prognozarea cererii viitoare și identificarea ineficiențelor.

În general, scopul urmăririi activelor este de a oferi organizațiilor datele în timp real de care au nevoie pentru a-și gestiona eficient activele, a îmbunătăți performanța lanțului de aprovizionare, a reduce costurile și a lua decizii informate cu privire la operațiunile lor. Folosind aceste informații, organizațiile își pot îmbunătăți operațiunile, își pot îmbunătăți experiența clienților și pot obține un avantaj competitiv în industria lor.

Perioada de timp estimată pentru a obține avantaje

Perioada de timp estimată pentru a crea valoare din soluțiile de urmărire a activelor va depinde de nevoile specifice ale organizației și de complexitatea soluției de urmărire a activelor care este implementată. Cu toate acestea, în multe cazuri, organizațiile se pot aștepta să vadă beneficiile urmăririi activelor în decurs de câteva luni până la un an de la implementare.

Pe termen scurt, urmărirea activelor poate oferi beneficii imediate, cum ar fi reducerea riscului de pierdere sau furt a activelor, îmbunătățirea acurateței inventarului și optimizarea utilizării activelor. Aceste beneficii pot fi obținute relativ rapid, adesea în câteva săptămâni sau luni de la implementare.
Pe termen lung, valoarea creată de urmărirea activelor poate crește pe măsură ce organizația câștigă o vizibilitate mai bună asupra operațiunilor lanțului de aprovizionare și identifică oportunități de optimizare și îmbunătățire. Acest lucru poate duce la economii suplimentare de costuri, o mai mare satisfacție a clienților și o eficiență îmbunătățită.

Pe măsură ce tehnologia continuă să evolueze și soluțiile de urmărire a activelor devin mai avansate, potențialul de creare de valoare va continua să crească. Învățarea automată și analiza predictivă, de exemplu, pot fi utilizate pentru a identifica modele și tendințe în mișcările activelor, permițând organizațiilor să anticipeze întreruperile din lanțul de aprovizionare și să ia măsuri preventive.

În general, intervalul de timp estimat pentru a crea valoare din soluțiile de urmărire a activelor va varia în funcție de nevoile specifice ale organizației. Cu toate acestea, prin implementarea unei soluții de

urmărire a activelor, organizațiile se pot aștepta să vadă un impact pozitiv asupra operațiunilor, eficienței și profitului lor într-un interval de timp relativ scurt.

3.7 Monitor de prezenţă pentru studenţi

Scop

Sistemul de prezență este un sistem care este utilizat pentru a urmări prezența unei anumite persoane și este aplicat în industrii, școli, universități sau locuri de muncă. Modul tradițional de a lua prezența are un dezavantaj, adică datele din lista de prezență nu pot fi reutilizate, iar urmărirea prezenței elevilor este mai dificilă. Sistemul de prezență bazat pe tehnologie, cum ar fi senzorii și sistemul de prezență bazat pe biometrie, a redus implicarea umană și erorile. Astfel, în această lucrare este prezentat un sistem de prezență bazat pe NFC. Un studiu comparativ între acest NFC și RFID este, de asemenea, discutat amănunțit, în special în ceea ce privește arhitecturile, caracteristicile de funcționalitate, beneficiile și punctele slabe ale acestora. Per total, atât sistemul de prezență NFC cât și RFID măresc eficiența în înregistrarea prezenței, sistemul NFC oferă mai multe facilități și o infrastructură mai ieftină atât în ceea ce privește costul operațional, cât și cel de instalare.

Perioada de timp estimată pentru a obţine avantaje

3 – 6 luni

3.8 Gestionarea automată a spaţiilor de lucru şi instalaţiilor asociate

Scop

Scopul managementului automatizat al spaţiilor de lucru şi instalaţiilor asociate este de a utiliza tehnologia pentru a eficientiza și automatiza procesele de management al clădirilor și spaţiilor de lucru pentru a îmbunătăți eficiența operațională, a reduce costurile și a spori experiența ocupantului clădirii. Aceasta include utilizarea tehnologiilor pentru clădirile inteligente care permit monitorizarea, controlul și optimizarea diferitelor sisteme de clădire, inclusiv HVAC, iluminat, securitate și utilizarea energiei.

Unele dintre obiectivele cheie ale managementului automatizat al spaţiilor de lucru şi instalaţiilor asociate includ:

- Eficiență operațională îmbunătățită: prin automatizarea proceselor de management al instalațiilor, organizațiile pot reduce timpul și resursele necesare pentru a-și gestiona unitățile, permițându-le să se concentreze mai mult pe activitățile de bază ale afacerii.
- Costuri reduse: Managementul automatizat al instalațiilor poate ajuta organizațiile să reducă consumul de energie, să minimizeze costurile de întreținere și să optimizeze alocarea resurselor.

- Performanță îmbunătățită a clădirii: prin valorificarea analizei datelor și a monitorizării în timp real, sistemele automate de management al instalațiilor pot detecta și rezolva mai rapid problemele de performanță a clădirii, rezultând o performanță mai bună a clădirii și costuri de operare mai mici.
- Experiență îmbunătățită a ocupanților: gestionarea automată a instalațiilor poate îmbunătăți experiența ocupanților, oferind medii mai confortabile și mai sigure prin monitorizarea și optimizarea în timp real a diferitelor sisteme de clădire.
- Conformitate: prin automatizarea și standardizarea proceselor, managementul automatizat al instalațiilor poate ajuta organizațiile să respecte reglementările și liniile directoare, reducând riscurile de amenzi, penalități și litigii.

În general, obiectivul managementului automatizat al facilităților este de a folosi tehnologia pentru a permite organizațiilor să realizeze un management general mai bun al clădirilor și facilităților lor. Prin sporirea eficienței, reducerea costurilor și îmbunătățirea experienței ocupanților, organizațiile pot deveni mai competitive și pot servi mai bine clienții.

Perioada de timp estimată pentru a obține avantaje

Perioada de timp estimată pentru a crea valoare din managementul automatizat al instalațiilor va depinde de mai mulți factori, cum ar fi dimensiunea și complexitatea clădirii sau a instalației, tipul de tehnologie utilizată și obiectivele specifice ale organizației.

În multe cazuri, organizațiile se pot aștepta să vadă beneficii măsurabile din sistemele lor automate de management al instalațiilor în decurs de câteva luni până la un an de la implementare. Aceste beneficii pot include:

- Consum redus de energie: Managementul automatizat al instalațiilor poate optimiza diverse sisteme de clădire, reducând consumul de energie și ducând la facturi mai mici la energie.
- Procese de întreținere eficientizate: prin automatizarea proceselor de întreținere, organizațiile pot reduce nevoia de intervenție manuală, pot economisi timp și pot reduce costurile.
- Experiență îmbunătățită a ocupanților: gestionarea automată a instalațiilor poate îmbunătăți nivelul de confort al clădirii, rezultând o satisfacție sporită a ocupanților.
- Eficiență operațională mai bună: Managementul automatizat al instalațiilor poate eficientiza diferite procese de management al clădirilor, rezultând o eficiență îmbunătățită și costuri organizaționale reduse.
- Întreținere predictivă: prin adoptarea întreținerii predictive, organizațiile pot îmbunătăți durata de viață a sistemelor lor de clădiri și pot reduce costurile de reparație.

În general, intervalul de timp estimat pentru a crea valoare din managementul automatizat al instalațiilor va depinde de nevoile specifice ale organizației și de complexitatea sistemelor care urmează să fie implementate. Oricum, prin valorificarea beneficiilor.

3.9 Automatizarea sarcinilor folosind servicii bazate pe cloud: motor de recomandare a unor produse

Scop

Analiza coșului de piață este o tehnică de modelare bazată pe teoria conform căreia, dacă cumpărați un anumit grup de articole, este mai mult (sau mai puțin) probabil să cumpărați un alt grup de articole. În comerțul cu amănuntul, majoritatea achizițiilor sunt cumpărate din impuls. Analiza coșului de piață oferă informații despre ce ar fi cumpărat un client dacă i-ar fi venit ideea.

Perioada de timp estimată pentru aplicaţie

1 – 6 luni

3.10 Înregistrări de rezervă / Dezastre naturale

Scop

Deținerea unui sistem automat pentru copierea de rezervă a datelor critice în mai multe regiuni diferite pentru a minimiza riscul pierderilor catastrofale, astfel încât, dacă există o defecțiune într-o întreagă regiune, inregistrarile de rezerva (back-up-urile) nu ar fi afectate, spre deosebire de crearea de backup-uri pe servere diferite din aceeași regiune, unde o defecțiune totală din regiune ar duce la pierderea de date chiar și cu backup-urile.

Perioada de timp estimată pentru a obţine avantaje

N /A

3.11 Chatbot pentru indicarea locurilor libere în parcările publice dintr-un oraş

Scop

O problemă cu care se confruntă toți șoferii de mașini este nevoia de a găsi locuri libere în parcările publice din oraș cât mai aproape de locul unde ne dorim să mergem. Acest lucru este destul de dificil deoarece șoferul se află în trafic și trebuie să se orienteze în funcție de situația din zonă.

O soluție care rezolvă problema și ușurează sarcina șoferului este o aplicație de tip chatbot pe telefonul

mobil al șoferului. Șoferul comunică cu aplicația prin voce și află în prealabil situația cu locuri de parcare libere în parcările situate în apropierea zonei în care șoferul are probleme de rezolvat.

Perioada de timp estimată pentru a obține avantaje

1 lună și jumătate – 10 luni

3.12 Chatbot pentru personalizarea activității de învățare a elevilor din învățământul liceal profesional

Scop

În mod clasic, elevii învață citind lecția scrisă pe hârtie sau citind lecția scrisă în format electronic într-un fișier word sau fișiere similare (pdf etc.). Lecția este de obicei urmată de un set de întrebări prin care elevul poate verifica modul în care a învățat lecția.

Aplicația care este propusă acum ajută elevul să învețe într-un mod interactiv cu mai multă eficiență.

Perioada de timp estimată pentru a obține avantaje

1 luna – 6 luni

3.13 Chatbot pentru studenții din instituția EDU

Scop

In ultima vreme multe companii de software încearcă să creeze cel puțin un chatbot bazat pe întrebări frecvente/întrebări și răspunsuri. Lucrările recente arată că este foarte ușor să construiești un bot, în timp ce să construiești unul inteligent ar putea fi extrem de greu (și costisitor). Boții specifici domeniului, cum ar fi boții de asistență a Centrului de automatizare bazati pe inteligența artificială, ar trebui să se considere interoperabili la mai multe nivele dar cu fiecare nou nivel, nivelul de complexitate crește exponențial. În ultimii ani, aplicațiile de mesagerie au depășit rețelele sociale și au devenit platformele dominante pe telefoanele inteligente. Acest potențial enorm ar trebui luat în considerare pentru a rezolva una dintre problemele pe care le are orice organizație mai mare de 10 participanți. Combinând diversele surse de date interne și externe existente la care compania are deja acces, majoritatea întrebărilor de la biroul de asistență de linia întâi și a doua ar putea fi rezolvate înainte de a veni în sprijin personalul de service. Automatizarea proceselor robotizate (RPA) este unul dintre cele mai fierbinți subiecte în rândul experților în procese pentru afaceri, în timp ce unul dintre domeniile cu cea mai rapidă creștere ale RPA este Knowledge Mining (exploatarea cunoştinţelor), care este aplicabil în special în mediul educațional (EDU), precum orice tip de sistem de sprijin pentru EDU.

Perioada de timp estimată pentru a obține avantaje

3 – 9 luni

3.14 E-learning bazat pe cloud

Scop

Cercetările în creștere în domeniile tehnologiei informației au un impact pozitiv în lumea educației. Implementarea e-learning-ului este una din contribuțiile tehnologiei informației la lumea educației. Implementarea e-learning-ului a fost implementată de mai multe instituții de învățământ din Indonezia. E-Learning oferă multe beneficii, cum ar fi flexibilitatea, diversitatea, măsurarea și așa mai departe. Aplicațiile actuale de e-learning au necesitat investiții mari în sisteme de infrastructură, indiferent de aplicația de e-learning comercială sau open-source. Dacă instituția ar avea tendința de a utiliza aplicația de e-learning cu sursă deschisă, ar avea nevoie de costuri mai mari pentru a angaja personal profesionist pentru întreținerea și actualizarea aplicației de e-learning. Poate fi o provocare să implementezi e-learning în instituțiile de învățământ. O altă problemă care poate apărea astăzi în tendința de utilizare a e-learning-ului este mai probabil ca instituția să își construiască propriul sistem de e-learning. Dacă două sau mai multe instituții sunt dispuse să construiască și să utilizeze un e-learning, astfel încât să poată minimiza cheltuielile pentru dezvoltarea sistemului și partajarea materialelor de învățare, acest lucru este mai probabil să se întâmple. Această lucrare discută starea actuală și provocările în e-learning și apoi explică conceptul de bază și arhitecturile anterioare propuse de cloud computing. În această lucrare, autorii au propus și un model de e-learning bazat pe cloud, care constă din cinci straturi, și anume: (1) stratul de infrastructură; (2) strat de platformă; (3) strat de aplicare; (4) strat de acces și (5) stratul utilizator. În plus față de această lucrare, am ilustrat și paradigma de schimbare de la e-learning convențional la e - learning bazat pe cloud și am descris beneficiile așteptate prin utilizarea e-learning-ului bazat pe cloud.

Perioada de timp estimată pentru a obține avantaje

6 – 12 luni

3.15 Comunicare/ Aplicație pentru schimbul de informații/ Canale

Scop

Scopul aplicațiilor de comunicare/schimb de informații este de a permite comunicarea și schimbul de informații eficient şi fără întreruperi între indivizi sau grupuri. Aceste aplicații oferă utilizatorilor o platformă pentru a se conecta cu alții, a colabora și a accesa informații în timp real, indiferent de locația lor.

Cu aplicațiile de comunicare/schimb de informații, utilizatorii pot partaja documente, fișiere și alte forme de date, pot organiza conferințe audio și video, transmite instantaneu mesaje și partaja ecrane. Scopul final este de a mări productivitatea, de a spori colaborarea și de a eficientiza fluxurile de lucru.

În plus, aceste aplicații oferă adesea caracteristici de securitate, cum ar fi criptarea de la un capăt la celălalt (end-to-end) pentru a proteja informațiile sensibile. Unele aplicații de comunicare/schimb de informații includ și funcții bazate pe inteligența artificială, cum ar fi traducerea documentelor, analiza sentimentelor și transcrierea automată, pentru a face comunicarea mai eficientă și mai efectivă.

În general, scopul aplicațiilor de comunicare/schimb de informații este de a facilita comunicarea și colaborarea eficientă, conducând la performanțe îmbunătățite, satisfacție sporită a clienților și profitabilitate mărită pentru întreprinderi și organizații.

Perioada de timp estimată pentru a obține avantaje

Perioada de timp estimată pentru a obtine avantaje pentru o aplicație de comunicare/schimb de informații poate varia în funcție de mai mulți factori, inclusiv de complexitatea aplicației, scopul de aplicare și tehnologia utilizată pentru dezvoltarea acesteia.

Pentru aplicațiile mai mici cu funcționalități limitate, avantajele pot fi obținute în câteva săptămâni sau luni. Astfel de aplicații pot fi o simplă platformă de mesagerie sau de partajare a fișierelor care are ca scop conectarea lucrătorilor de la distanță sau colegilor de echipă.

Pentru aplicații mai mari cu funcționalități complexe, cum ar fi apeluri video de grup, table interactive, utilizarea documentelor în comun și alte funcții avansate, poate dura câteva luni sau chiar ani pentru a obține avantaje.

Timpul de dezvoltare va depinde, de asemenea, de resursele echipei, de experiența și de metodologia utilizată în construirea aplicației. Metodologia vioaie care implică dezvoltare iterativă și feedback regulat din partea utilizatorilor poate ajuta la scurtarea ciclului de viață al dezvoltării și la crearea rapidă de avantaje.

În general, o aplicație de comunicare/schimb de informații poate crea valoare de îndată ce devine operațională și începe să uşureze colaborarea eficientă și să îmbunătățească productivitatea utilizatorilor. Cheia este să vă concentrați pe crearea unei aplicații care să răspundă nevoilor utilizatorilor, să fie ușor de folosit și să ofere o experiență satisfăcătoare care îi va determina să utilizeze aplicația pe termen lung.

3.16 Monitorizarea continuă a funcţionării unor instalaţii industriale folosind tehnologii cloud computing şi IoT

Scop

Instalatiile industriale care apartin unor firme pot prezenta un pericol daca valorile unor parametri ce caracterizeaza aceste instalatii se află in afara domeniului de funcţionare normală.

Un exemplu este rezervorul de depozitare care conține amestecul lichefiat propan-butan care este folosit pentru a propulsa lichidul din interiorul recipientelor de pulverizare.

Acest gaz este îmbuteliat în recipiente mai mici împreună cu lichidul de pulverizat prin apăsarea unui buton. Aplicația monitorizează anumite mărimi (presiunea gazului, temperatura rezervorului etc.) ale instalației.

Când parametrii monitorizați se apropie de valori periculoase, se iau măsuri pentru a aduce funcționarea instalației la parametri normali.

Perioada de timp estimată pentru a obţine avantaje

3 saptamani - 4 luni

3.17 Monitorizarea continuă a pacientului

Scop

Un sistem care utilizează senzori împreună cu hub-ul IoT care poate monitoriza de la distanță elementele vitale ale pacientului și poate transmite avertismente dacă anumite mărimi depășesc anumite praguri.

Perioada de timp estimată pentru a obţine avantaje

1 an – 1,5 ani

3.18 Crearea mediilor de testare

Scop

Furnizați și creați resursele necesare pentru a rula versiuni de testare ale implementărilor existente, astfel încât noile funcții sau posibile remedieri de erori să poată fi scrise și rulate fără a perturba implementarea curentă.

Perioada de timp estimată pentru a obține avantaje

1 săptămână

3.19 Crearea unei aplicații didactice pentru a ajuta elevii să învețe o limbă străină

Scop

Aplicația este dezvoltată în scopuri educaționale. Este concepută pentru a facilita învățarea unei limbi străine. Există limbi străine în care pentru fiecare sunet (fonem) care alcătuiește un cuvânt atunci când este pronunțat, este folosit același element grafic (grafem) pentru a înregistra cuvântul pronunțat în scris. În alte limbi, pentru același sunet, sunt folosite două sau trei combinații de elemente grafice pentru a fixa cuvântul în scris.

Pentru a uşura învățarea unei limbi străine, a fost introdus alfabetul fonemic internațional, care folosește întotdeauna același simbol grafic pentru a înregistra în scris același sunet vorbit. Acest lucru facilitează învățarea unei limbi străine.

Prin utilizarea aplicației, elevul poate învăța pronunția corectă a cuvintelor din limba străină de învățat.

Perioada de timp estimată pentru a obține avantaje

3 săptămâni – 3 luni

3.20 Copii de rezervă a datelor şi arhivarea lor

Scop

Backup. Arhiva. Metodă de stocare a datelor. Datele originale rămân la locul lor, în timp ce o copie de rezervă este stocată într-o altă locație . Datele arhivate sunt mutate din locația inițială într-o locație de stocare a arhivei.

Trăind într-o lume în care criminalitatea cibernetică este la ordinea zilei. Nici o zi nu trece fără cazuri de pierderi majore de date, care uneori devin fatale pentru un număr destul de mare de afaceri.

Metodele tradiționale de backup a datelor s-au dovedit eficiente în salvarea datelor pentru o lungă perioadă de timp. Cu toate acestea, datele sunt predispuse la viruși și, datorită naturii lor portabile, se pot pierde și reprezintă o amenințare pentru afacerile moderne.

Backup-ul și arhivarea bazate pe cloud reprezintă o soluție pentru aceste provocări. Este ușor de implementat și oferă securitate maximă a datelor. Cu această abordare, puteți face backup sau arhiva

fișierele dvs. sensibile în sisteme de stocare bazate pe cloud. Acest lucru oferă asigurarea că datele dvs. sunt încă intacte, chiar dacă datele dvs. live devin într-un fel compromise.

Unele servicii de cloud computing vă permit să programați copii de rezervă pentru a vă satisface nevoile unice. În plus, vă puteți cripta backup-urile din cloud și face imposibil accesul hackerilor și al hoţilor.
Cu stocarea în cloud, puteți obține atât de mult spațiu cât aveți nevoie și puteți stoca atât de multe date câte doriţi și veți plăti doar pentru ceea ce utilizați de fapt.

Perioada de timp estimată pentru a obţine avantaje

Perioada de timp pentru obţinerea avantajelor poate varia în funcție de nevoile specifice ale organizației și de nivelul de implementare a backup-ului și arhivei, dar beneficiile pot începe să se acumuleze încă de la prima implementare.

3.21 Sistem bazat pe cloud pentru prevenirea pierderii datelor

Scop

DLP (Data Loss Prevention) este un instrument de securitate pentru protecția datelor, dar complexitatea și progresul tehnologic al acestuia contribuie la o înțelegere foarte mică a funcționalității și capacităților instrumentului. Cu diferite nume și abordări tehnologice, poate fi dificil să înțelegem valoarea finală a instrumentului și cea care se potrivește cel mai bine mediilor. Există o înțelegere diversă a ceea ce este soluția DLP. Unii oameni consideră că acest DLP criptează sau controlează intrarea USB, în timp ce alții privesc mai departe.

DLP-ul este definit ca: produs care, bazat pe politici centrale, identifică, monitorizează și protejează stagnarea, mișcarea și utilizarea datelor printr-o analiză profundă a conținutului acestora. Caracteristicile cheie ale DLP-ului sunt:
1. analiza de conţinut;
2. managementul politicii centrale;
3. acoperă conținut pe mai multe platforme și locații.
Soluțiile DLP protejează datele sensibile și ajută organizațiile să-și înțeleagă mai bine datele și să-și îmbunătățească capacitatea de a gestiona conținutul.

Perioada de timp estimată pentru a obţine avantaje

6 – 12 luni

3.22 Sistem de management al datelor despre angajații unei companii

Scop

În general, companiile mici cu un număr mic de angajați gestionează datele angajaților folosind fișiere excel sau word în care creează tabele. Datele angajaților sunt înscrise în aceste tabele. Aceste tabele nu au un format unitar și modificarea unor date despre angajați necesită uneori efectuarea de modificări în mai multe fișiere.

Când se fac modificări, este posibil ca unele fișiere să nu fie modificate, iar în alte fișiere, date importante despre angajați pot fi distruse accidental. În plus, accesarea informațiilor despre un angajat necesită vizualizarea tuturor documentelor Excel sau Word.

Aplicația propusă oferă posibilitatea stocării datelor angajaților într-o bază de date relațională stocată fie pe propriul server, fie pe serverul altei companii. În plus, interfața grafică folosită este prietenoasă și sugestivă.

Perioada de timp estimată pentru a obține avantaje

2 săptămâni - 2 luni

3.23 Certificarea activelor digitale folosind registru distribuit/ blockchain

Scop

Principalele caracteristici ale blockchain-ului sunt transparența și descentralizarea, cu care sistemele de astăzi nu se pot lăuda. Identitatea digitală combinată cu tehnologia blockchain va permite oamenilor să îndeplinească sarcini mai rapide, mai simple și mai sigure, inclusiv dovezi de identitate, fapte, stare și date. Incredibil, adevărul este că căutarea de noi angajați, verificarea datelor candidaților și a cererii de angajare în sine ar putea fi un proces care ar necesita doar câteva clicuri de mouse pe computer, cu datele obținute în cea mai mare siguranță. Dar blockchain-ul doar oferă. Prin plasarea tuturor informațiilor despre identitatea noastră pe el, cu o criptare care face totul sigur și transparent și întotdeauna accesibil prin internet, cheltuim tot timpul petrecut pentru a dovedi identitatea, datele, faptele, starea afacerilor si cele mai importante lucruri. Imaginați-vă că la cererea de afaceri putem atașa și 3 chei criptografice, astfel încât angajatorul să verifice cu ușurință cu certitudinea absolută că am absolvit efectiv facultatea pe care am precizat-o în CV, dacă suntem nemulțumiți și dacă la urma urmei suntem persoana care pretinde că este. Acest proces ar dura aproximativ câteva minute, în timp ce același proces durează câteva zile, dacă nu săptămâni, deoarece verificarea datelor se face prin scrierea de interogări în fiecare dintre aceste sisteme din care provin datele.

Perioada de timp estimată pentru a obține avantaje

3 – 9 luni

3.24 Identitate digitală

Scop

Identitatea este foarte valoroasă pentru noi, și nu pentru instituții, iar noi nu ne comportăm în consecință. Din cauza lipsei de conștientizare și educație despre identitatea în sine, din cauza centralizării digitale și fizice a bazelor de date și a datelor despre identitățile noastre, care creează slăbiciuni inevitabile care subminează valoarea sistematică a datelor noastre personale. Sistemele centralizate sunt o pradă bună pentru atacatorii cu intenții rele, deoarece, dacă pătrund în sistem, pot fura (copia) cu ușurință cantități mari de date stocate în acel sistem. Am asistat la o mulțime de atacuri asupra sistemelor centralizate, nu a sistemelor de afaceri mici, ci a companiilor mari și influente la nivel global, cum ar fi Yahoo, eBay, Adobe, JP Morgan Chase, Sony și multe altele.

Blockchain oferă soluția acestei probleme care devine din ce în ce mai persistentă din cauza nevoilor constante, a cererii crescute și a utilizării identității digitale. Dar, așa cum am menționat mai devreme, aceasta este o tehnologie nouă și se află abia în fazele incipiente ale proiectului și încă investigăm toate posibilitățile și aplicarea acestei tehnologii. Cu nevoia de a ne demonstra identitatea, ne întâlnim în fiecare zi și în locuri diferite. La serviciu, la bancă, într-un magazin, în călătorii, în instituții de stat și în multe locuri diferite. În prezent există multe proiecte noi și viitoare și companii tinere care se confruntă cu această problemă și încearcă să-și găsească locul pe piață. În această parte vom menționa unele dintre ele și le vom explica mai precis modelele de afaceri.

Perioada de timp estimată pentru a obține avantaje

1-3 luni

3.25 Digital twinning (reprezentarea virtuală a unui sistem)

Scop

Creați un mediu virtual bazat pe un sistem din lumea reală, folosind senzori și capacitățile IoT și explorați posibilitățile și consecințele schimbării mediului, monitorizând starea de sănătate a sistemelor, astfel încât întreținerea și reparațiile să poată fi efectuate pe măsură ce apare nevoia, mai degrabă decât inspecțiile programate.

Prin observarea datelor adunate de la senzori, puteți simula schimbările în mediu pentru a vedea cum va răspunde sistemul și pentru a obține perspective despre cum să îmbunătățiți performanța

sistemului. De exemplu, ar putea fi folosit pentru a îmbunătăți performanța unui sistem de ventilație printr-o utilizare mai dinamică, unde crește fluxul de lucru la orele de vârf și în zonele aglomerate și economisește energie atunci când este mai puțină nevoie, creând atât un mediu mai plăcut, cât și scăderea costurilor energetice.

Perioada de timp estimată pentru a obține avantaje

6 luni – 1 an

3.26 Platformă de prevenire a dezastrelor

Scop

Folosind dispozitive cu senzori de mediu compatibili cu internetul care trimit date către un server de analiză bazat pe cloud, se generează alarme și rapoarte bazate pe analiza datelor.

O soluție cuprinzătoare de monitorizare pentru colectarea, analizarea și răspunsul la telemetrie din mediile dvs. cloud și locale. Maximizarea disponibilității și performanței aplicațiilor și serviciilor dvs.

Colectarea și integrarea datelor de la fiecare strat și componentă a sistemului dvs. într-o platformă comună de date. Corelează datele pentru mai multe abonamente și chiriași, pe lângă găzduirea datelor pentru alte servicii. Deoarece aceste date sunt stocate împreună, pot fi corelate și analizate folosind un set comun de instrumente. Datele pot fi apoi utilizate pentru analiză și vizualizări pentru a vă ajuta să înțelegeți cum funcționează aplicațiile dvs. și să răspundă automat la evenimentele din sistem.

Perioada de timp estimată pentru a obține avantaje

Perioada de timp pentru a crea valoare pentru o astfel de platformă ar depinde de diverși factori, cum ar fi complexitatea platformei, resursele disponibile și nivelul de expertiză al echipei care dezvoltă platforma. În unele cazuri, valoarea unei platforme de prevenire a dezastrelor poate fi imediat evidentă, în timp ce în alte cazuri, poate dura ceva timp pentru a analiza și măsura eficacitatea acesteia. În cele din urmă, succesul și valoarea unei platforme de prevenire a dezastrelor ar depinde de capacitatea acesteia de a preveni sau de a atenua impactul dezastrelor.

3.27 Distribuirea coletelor într-o regiune geografică cu ajutorul dronelor autonome

Scop

Cu câteva secole în urmă, porumbeii dresați (numiți și porumbei călători) erau folosiți pentru a transmite mesaje între emițător și destinatar. Cel puțin așa spun poveștile care au ajuns la noi.

Au existat avantaje și dezavantaje ale acestui mod de transmitere a mesajelor. O modalitate de a transmite pachete între un punct de distribuție și diverși destinatari poate fi utilizarea dronelor autonome.

Perioada de timp estimată pentru a obține avantaje

3 săptămâni – 6 luni

3.28 Sistem de detectare a asemănării documentelor și extragere a informațiilor documentelor

Scop

Este o tendință umană de a formula ipoteze în timp ce se analizează dificultatea extragerii informațiilor în documente. Presupunem automat că este mai ușor să extragem informații sub formă de entități denumite dintr-un set de documente similare. Cu toate acestea, documentele asemănătoare au un set distinct de probleme. Entitățile denumite din aceste tipuri de documente variază ca dimensiune, asemănătoare cu numărul de caractere, cuvinte, înălțime, lățime și locație. Aceste variații nu pot fi gestionate folosind euristici sau modele de limbaj pre-antrenate.

Perioada de timp estimată pentru a obține avantaje

6 – 12 luni

3.29 Traducerea documentelor

Scop

Traducerea documentelor care conțin descrieri ale produselor vândute pe un site web, astfel încât afacerea să poată satisface un grup demografic mai larg și poate duce la un număr crescut de vânzări. Este deosebit de important să vă asigurați că un site web este disponibil în diferite limbi atunci când încercați să atrageți un public internațional sau compania furnizează o zonă sau o industrie care constă dintr-o mulțime de vorbitori care nu sunt majoritari.

Fiind într-un spațiu multilingv, poate fi, de asemenea, util să traduceți automat orice conținut generat de utilizatori, cum ar fi recenzii despre produse, sau să creați și să mențineți o bază de date cu întrebări frecvente în mai multe limbi diferite.

Perioada de timp estimată pentru a obține avantaje
3 luni – 6 luni

3.30 Găzduire site dinamic

Scop
Un mediu de găzduire web conține detalii specifice aplicației, cum ar fi locul unde este stocată aplicația și funcțiile și serviciile esențiale pentru gestionarea întregii aplicații. Cele mai comune tipuri de găzduire web sunt: găzduire statică, găzduire dinamică si găzduire locală.

Perioada de timp estimată pentru a obține avantaje
1 – 3 luni

3.31 Site web dinamic cu stocarea datelor într-o bază de date

Scop
Site-urile sunt foarte populare în zilele noastre și permit afișarea informațiilor într-un mod atractiv și prietenos. Informațiile conținute în aceste site-uri sunt sub formă de text sau imagini. Unele site-uri pot avea multe pagini în funcție de scopul lor. Adesea, informațiile pe care le transmit trebuie schimbate relativ des din cauza anumitor condiții.

De exemplu, o pizzerie care are o pagină web schimbă meniul zilnic. Pagina web trebuie actualizată zilnic. În acest caz, proprietarul pizzeriei (eu am ales o pizzerie ca exemplu, dar pot fi și alte exemple) trebuie să contacteze zilnic persoana care a realizat site-ul pentru a actualiza informațiile. Un site dinamic care afișează informații folosind o bază de date este binevenit.

Perioada de timp estimată pentru a obține avantaje
2 săptămâni - 1 lună

3.32 Aplicație de comerț electronic

Scop
Scopul principal al unei aplicații de comerț electronic este de a permite tranzacțiile comerciale electronice între afacerişti și consumatori prin internet. Aplicațiile de comerț electronic permit companiilor să-și vândă produsele și serviciile online, iar consumatorilor să cumpere acele produse și servicii prin internet.

Scopul unei aplicații de comerț electronic este de a oferi consumatorilor o experiență de cumpărături perfectă, oferind în același timp afaceriştilor o modalitate eficientă din punct de vedere al costurilor de a-și vinde produsele și serviciile. Aplicația ar trebui să fie proiectată pentru a fi intuitivă, ușor de utilizat și să ofere opțiuni de plată convenabile, permițând clienților să facă cumpărături cu ușurință.

În plus, o aplicație de comerț electronic ar trebui să fie proiectată pentru a oferi companiilor capacități solide de raportare și analiză, permițându-le să urmărească datele de vânzări, nivelurile de inventar, modelele de cumpărare ale clienților și alte valori cheie. Acest lucru ajută companiile să identifice tendințele și să ia decizii bazate pe date care promovează creșterea și succesul afacerii.

În general, scopul unei aplicații de comerț electronic este de a facilita achizițiile online sigure și convenabile, facilitând în același timp companiilor să își gestioneze tranzacțiile online. Oferind clienților o experiență de cumpărături simplificată, ușor de utilizat și companiilor cu instrumente de management eficiente, o aplicație de comerț electronic poate crește semnificativ vânzările, veniturile și cota de piață pentru companii.

Perioada de timp estimată pentru a obține avantaje

Perioada de timp pentru a crea valoare dintr-o aplicație de comerț electronic depinde de mai mulți factori, inclusiv dimensiunea și complexitatea aplicației, nivelul de personalizare necesar și resursele disponibile pentru dezvoltare.

De obicei, poate dura câteva luni până la un an pentru a proiecta, dezvolta, testa și lansa o aplicație de comerț electronic. Cu toate acestea, companiile pot începe să genereze valoare dintr-o aplicație de comerț electronic chiar înainte ca aceasta să fie complet finalizată, dacă urmează o abordare de dezvoltare agilă, care le permite să ofere clienților mici creșteri de valoare mai rapid.

În primele etape ale dezvoltării aplicațiilor de comerț electronic, companiile ar trebui să se concentreze pe crearea unui produs minim viabil (MVP) care oferă un set de bază de caracteristici și funcționalități pentru ca clienții să facă cumpărături online. Acest lucru permite companiilor să-și valideze ipotezele și să testeze piața înainte de a investi mai multe resurse în dezvoltarea de funcții suplimentare.

Odată ce MVP-ul este lansat, companiile pot începe să genereze valoare prin măsurarea unor valori cheie de performanță, cum ar fi traficul pe site-ul web, ratele de conversie și nivelurile de satisfacție a clienților. Ei pot folosi aceste date pentru a repeta și a îmbunătăți în mod continuu aplicația, adăugând noi caracteristici și funcționalități pentru a stimula implicarea clienților, vânzările și veniturile.

În general, în timp ce intervalul de timp estimat pentru a crea valoare dintr-o aplicație de comerț electronic poate depinde de diverși factori, companiile pot începe să-și realizeze beneficiile din primele

etape de dezvoltare și să-și îmbunătățească și să-și mărească continuu caracteristicile în timp pentru a stimula implicarea și creșterea clienților.

3.33 Catalog electronic cu rezultatele şcolare ale elevilor

Scop

Aplicația înregistrează într-o bază de date rezultatele obținute de liceeni la disciplinele studiate la școală. Aplicația analizează rezultatele fiecărui elev și atunci când rezultatele sunt sub limita de trecere sau sunt aproape de limită, sesizează acest lucru trimițând un e-mail sau un mesaj de avertizare pe telefonul mobil către părinții lor.

Perioada de timp estimată pentru a obţine avantaje

1 săptămână - 1 lună și jumătate

3.34 Controlul Accesului în Spaţiile de lucru

Scop

Scopul Controlului Accesului în Spaţiile de lucru este de a se asigura că numai persoanele autorizate au acces la o anumită locație fizică sau la o anumită unitate. Controlul accesului ajută la prevenirea accesului neautorizat, a furtului și a vandalismului și, de asemenea, poate ajuta la menținerea siguranței și securității angajaților. Prin implementarea măsurilor de control al accesului, o organizație poate proteja zonele sensibile ale unității de intrarea neautorizată, poate proteja activele și informațiile și poate reduce riscul de vătămare a angajaților.

Controlul accesului în spaţiile de lucru implică de obicei utilizarea unui sistem electronic care va solicita persoanelor autorizate să prezinte acreditări sau documente de identificare pentru a putea intra în zonele restricționate. Sistemul verifică acreditările prezentate cu o bază de date pentru persoane autorizate și acordă acces numai dacă acreditările prezentate se potrivesc cu o intrare autorizată în baza de date. Sistemele electronice de control al accesului pot fi configurate pentru a oferi acces la diferite niveluri de securitate. De exemplu, angajaților li se poate acorda acces la zone relevante pentru munca lor, în timp ce zonele extrem de sensibile pot necesita măsuri de securitate suplimentare, cum ar fi datele biometrice sau autentificarea dublă.

În general, scopul controlului accesului în spaţiile de lucru este de a oferi un mediu sigur pentru indivizi și active din cadrul unei organizații. Măsurile de control al accesului pot ajuta la reducerea riscului de deteriorare, furt și intrare neautorizată, precum și la îmbunătățirea încrederii și siguranței angajaților.

Perioada de timp estimată pentru a obține avantaje

Perioada de timp estimată pentru a crea valoare cu Controlul Accesului în Spaţiile de lucru depinde de implementarea și cerințele specifice ale organizației. Cu toate acestea, unele beneficii ale controlului accesului pot fi experimentate imediat, în timp ce altele pot dura mai mult pentru a se realiza.

Beneficiile imediate pot include securitate îmbunătățită și risc redus de furt, vandalism sau acces neautorizat. Acest lucru poate ajuta la protejarea activelor și a informațiilor valoroase, la menținerea siguranței angajaților și la creșterea încrederii generale și a liniștii sufletești.

Beneficiile pe termen lung, cum ar fi eficiența îmbunătățită și economiile de costuri, pot dura mai mult pentru a se realiza. De exemplu, un sistem automat de control al accesului poate simplifica procesul de verificare a drepturilor de acces și a permisiunilor, reducând cheltuielile administrative și erorile. De asemenea, poate ajuta la evitarea necesității de a angaja personal suplimentar pentru a securiza zonele restricționate. Aceste beneficii se pot adăuga în timp, contribuind la economii continue și la creșterea eficienței.

În general, intervalul de timp estimat pentru a crea valoare cu Controlul Accesului în Spaţiile de lucru depinde de implementarea specifică, de dimensiunea și complexitatea unității și de obiectivele de securitate și de control al accesului aparținând organizației. Cu toate acestea, controlul accesului este o investiție valoroasă în protejarea activelor valoroase, a informațiilor și a angajaților și în asigurarea unui mediu sigur și securizat.

3.35 Managementul spaţiilor de lucru şi al instalaţiilor asociate lor

Scop

Scopul managementului spaţiilor de lucru şi ale instalaţiilor asociate lor (Facilities Management (FM)) este de a asigura de faptul că mediul construit sprijină funcționarea eficientă a activităților de bază ale unei organizații prin furnizarea de măsuri sigure, funcționale și confortabile. În mod specific, obiectivele managementului facilităților pot include:

- Întreținere și întreținere: managementul spaţiilor de lucru şi ale instalaţiilor asociate lor urmărește să se asigure că mediul construit este întreținut, actualizat și reînnoit corespunzător, după cum și când este necesar.
- Optimizarea costurilor: managementul spaţiilor de lucru şi ale instalaţiilor asociate lor se preocupă de optimizarea furnizării serviciilor associate acestuia și de a obține un raport calitate-preț, asigurând în același timp menținerea standardelor de înaltă calitate a serviciilor.
- Managementul activelor: managementul spaţiilor de lucru şi ale instalaţiilor asociate lor implică adesea gestionarea activelor fizice ale unei organizații, inclusiv structurile de construcție,

echipamentele și utilajele, asigurându-se că acestea sunt utilizate în mod optim și generând rentabilitatea investiției.

- Performanța clădirii: managementul spaţiilor de lucru şi ale instalaţiilor asociate lor se concentrează pe îmbunătățirea standardelor de performanță a clădirii, cum ar fi siguranța, eficiența energetică, performanța de mediu și eficiența întreținerii.
- Satisfacția și productivitatea ocupanților: managementul spaţiilor de lucru şi al instalaţiilor asociate lor își propune să ofere un mediu sigur și confortabil pentru ocupanții clădirii, promovând un sentiment de bunăstare și implicare cu spațiile de lucru interioare și exterioare.

Pe scurt, scopul managementul spaţiilor de lucru şi ale instalaţiilor asociate lor este de a gestiona și optimiza mediul construit, susținând activitățile organizaționale, sporind valoarea activelor fizice, optimizarea resurselor și asigurarea confortului și satisfacției utilizatorilor.

Perioada de timp estimată pentru a obţine avantaje

Perioada de timp estimată pentru a crea valoare din gestionarea spaţiilor de lucru şi ale instalaţiilor asociate lor depinde de mai mulți factori, inclusiv de starea infrastructurii actuale a instalațiilor, de obiectivele organizației și de disponibilitatea resurselor. Iată câteva exemple:

- Întreținere și reparaţii: Reparaţiile și întreținerea regulată a infrastructurii instalațiilor pot ajuta la prelungirea duratei de viață a acesteia, la reducerea timpului de nefuncționare și la evitarea reparațiilor costisitoare. Valoarea poate fi realizată pe termen scurt și mediu, în funcție de amploarea întreținerii necesare, de complexitatea sistemelor și de disponibilitatea resurselor.
- Îmbunătățiri ale eficienței energetice: Managementul spaţiilor de lucru şi ale instalaţiilor asociate lor include adesea inițiative care vizează reducerea consumului de energie și promovarea practicilor durabile. Aceste inițiative pot ajuta la reducerea costurilor cu energia, la îmbunătățirea performanței de mediu și la îndeplinirea cerințelor de conformitate. Valoarea îmbunătățirii eficienței energetice poate fi realizată pe termen mediu și lung, deoarece acestea necesită adesea investiții mai substanțiale și implementarea de soluții complexe.
- Performanța clădirii: Managementul spaţiilor de lucru şi ale instalaţiilor asociate lor implică, de asemenea, îmbunătățirea standardelor de performanță a clădirii, cum ar fi siguranța, performanța de mediu și eficiența întreținerii. Valoarea îmbunătățirii performanței clădirii poate fi realizată pe termen lung, deoarece acestea implică adesea planificare pe termen lung, investiții și implementare de soluții.

În general, intervalul de timp estimat pentru ca managementul spaţiilor de lucru şi ale instalaţiilor asociate lor să creeze valoare variază în funcție de obiectivele specifice și contextul organizației. Cu toate acestea, un program de management al spaţiilor de lucru şi ale instalaţiilor asociate lor bine executat poate oferi beneficii imediate, cum ar fi reducerea costurilor operaționale, îmbunătățirea

siguranței și îmbunătățirea experienței utilizatorului, ceea ce poate duce la economii de costuri pe termen lung și îmbunătățiri ale productivității.

3.36 Date despre ocuparea spaţiilor de lucru şi ale instalaţiilor asociate lor

Scop

Datele de ocupare ajută la abordarea nevoilor ocupanților oricărui spațiu de lucru/zonă/instalație prin furnizarea de informații echipei de management al spaţiilor de lucru care se ocupă cu curățenia la cerere, în spaţii cu mese de birou comune etc., reumplerea stocurilor în zonele frecvent utilizate, cum ar fi docurile de cafea.

Dispozitive care raportează la un centru de monitorizare bazat pe cloud , care numără persoanele care intra si care ies dintr-o anumită clădire sau locație, pentru ca managementul să ia decizii informate pentru managementul angajaților, cifra de afaceri, succesul campaniei de marketing etc.

Perioada de timp estimată pentru a obţine avantaje

Datele privind ocuparea managementul spaţiilor de lucru şi ale instalaţiilor asociate pot crea valoare imediat din momentul implementării. Cu toate acestea, valoarea creată poate varia în funcție de natura datelor de ocupare, de tipul unității și de modul în care datele de ocupare sunt analizate și utilizate.

Unele beneficii care pot fi realizate imediat după implementare includ:

- Eficiență: datele privind ocuparea spaţiilor de lucru şi ale instalaţiilor asociate pot ajuta organizațiile să identifice spațiile subutilizate și să le optimizeze utilizarea. Acest lucru poate reduce risipa de energie și costurile de întreținere.
- Productivitate: Utilizarea datelor privind ocuparea pentru a înțelege utilizarea spațiului poate oferi o perspectivă asupra eficienței spațiilor de colaborare, oferind angajaților spații care ajută la productivitate și creează o atmosferă pentru a intra în zonă.
- Reducerea costurilor: Datele precise privind ocuparea îmbunătățesc luarea deciziilor, permițând întreprinderilor să reducă dimensiunea și cheltuielile instalațiilor care sunt subutilizate.
- Beneficii pentru mediu: Utilizarea eficientă a datelor privind ocuparea instalațiilor poate reduce emisiile de carbon și poate promova durabilitatea mediului.

Valoarea datelor privind ocuparea spaţiilor de lucru şi ale instalaţiilor asociate continuă să evolueze în timp. Cu colectarea și analiza continuă a datelor, datele de ocupare pot fi utilizate pentru a optimiza utilizarea spațiului, a deduce modele de cerere și a reduce costurile. Mai mult decât atât, pe măsură ce

datele de pe mai multe site-uri sunt agregate, pot fi generate informații mai ample despre modelele de utilizare în diferite facilități.
În general, intervalul de timp estimat pentru a crea valoare din datele privind ocuparea spaţiilor de lucru şi ale instalaţiilor asociate depinde de diferiți factori, inclusiv dimensiunea și complexitatea spaţiilor de lucru şi ale instalaţiilor asociate, instrumentele analitice utilizate și cultura internă a organizației față de luarea deciziilor bazate pe date.

3.37 Comparea fişierelor

Scop

Scopul comparării fișierelor este de a găsi și evidenția diferențele dintre conținutul a două sau mai multe fișiere. Fișierele pot fi în diferite formate, cum ar fi documente text, foi de calcul sau programe. Compararea fișierelor se face de obicei pentru a:

- Verifica precizia: compararea fișierelor poate ajuta la validarea faptului că datele au fost importate sau exportate corect. De exemplu, compararea unui fișier sursă cu un fișier țintă după migrarea datelor poate ajuta la confirmarea faptului că toate datele au fost transferate cu precizie.
- Asigura coerența: compararea mai multor versiuni ale unui fișier poate ajuta la asigurarea coerenței între diferitele versiuni. De exemplu, compararea a două versiuni ale unui program software poate ajuta la identificarea oricăror diferențe sau erori în cod.
- Identifica modificările: compararea a două versiuni ale unui document poate ajuta la identificarea modificărilor care au fost făcute între ele. Acest lucru poate fi util pentru urmărirea revizuirilor, colaborarea la documente sau pentru identificarea plagiatului.
- Rezolva conflictul: compararea a două versiuni diferite ale unui fișier poate ajuta la detectarea oricăror conflicte între ele, cum ar fi la îmbinarea modificărilor de cod făcute de diferiți dezvoltatori într-un sistem de control al versiunilor.

În general, scopul comparării fișierelor este de a se asigura că fișierele sunt corecte, consecvente și actualizate și de a identifica orice modificări sau erori care pot exista între mai multe versiuni ale unui fișier.

Perioada de timp estimată pentru a obţine avantaje

Perioada de timp estimată pentru a crea valoare din compararea fișierelor depinde de obiectivele și contextul specific. Iată câteva exemple:

- Compararea codului software: în acest caz, compararea fișierelor poate ajuta la identificarea problemelor și inconsecvențele în cod, ajutând la eforturile de depanare și testare. Valoarea

poate fi realizată relativ rapid, în funcție de complexitatea codului și de numărul de fișiere care trebuie comparate.

- Compararea fișierelor de date: compararea fișierelor de date poate ajuta la asigurarea acurateței datelor și la controlul calității datelor. Perioada de timp estimată pentru crearea valorii depinde de dimensiunea fișierelor de date, de complexitatea procesului de comparare și de nivelul de validare necesar.
- Compararea versiunilor de document: compararea versiunilor de document poate ajuta la identificarea modificărilor făcute de diferiți autori și la asigurarea coerenței între versiuni. Perioada de timp estimată pentru a crea valoare depinde de complexitatea documentului și de numărul de versiuni care trebuie comparate.

În general, intervalul de timp estimat pentru a crea valoare din compararea fișierelor poate varia foarte mult în funcție de cazul de utilizare specific și de complexitatea fișierelor comparate. Cu toate acestea, compararea fișierelor poate oferi beneficii imediate, cum ar fi identificarea erorilor sau inconsecvențelor, care pot duce la economii de timp și costuri pe termen lung.

3.38 Sistem de stocare a fişierelor folosind criptografie hibridă cloud computing

Scop

Tehnologia cloud a fost folosită în mai multe domenii, producție și academii de apărare, pentru a furniza cantități masive de informații. Informații extrase din cloud la cererea clientului. O serie de provocări ar trebui rezolvate pentru a păstra informațiile în sistem. Pentru a salva datele în cloud, trebuie abordate mai multe provocări. O serie de tehnici ar putea fi utilizate în rezolvarea conflictelor. În acest articol, am propus o steganografie hibridă și o metodă de criptare pentru securitatea datelor. În aplicațiile de internet, utilizarea unei soluții optime nu era potrivită pentru protecția la nivel înalt a informațiilor. Am introdus o nouă tehnică de securitate pe criptografia cu cheie simetrică și Steganografia. Rivest cipher 6 (RC6), Advanced Encryption Standard (AES), Byte Rotation Algorithm (BRA) și tehnicile blowfish pentru a furniza informații de siguranță a blocului, iar lungimea cheii tehnice a fost de 128 de biți. A fost aplicat un algoritm de steganografie de securitate critică a datelor, Least Signification Bit (LSB).

Perioada de timp estimată pentru a obține avantaje

1 – 3 luni

3.39 Gestionarea vârfurilor de trafic

Scop

Scopul gestionării vârfurilor de trafic este de a vă asigura că site-ul sau aplicația dvs. poate face față creșterilor bruște ale traficului fără a încetini sau a se prăbuși.

Perioada de timp estimată pentru a obține avantaje

Timpul necesar pentru a crea valoare din gestionarea vârfurilor de trafic depinde de complexitatea infrastructurii, de numărul de utilizatori și de obiectivele specifice ale organizației. Cu toate acestea, organizațiile pot vedea beneficii imediate în ceea ce privește performanța și fiabilitatea îmbunătățite.

3.40 Găzduire site web static folosind AWS (sau alte rețele cloud)

Scop

Tendința de a găzdui site-uri web statice pe Amazon S3 devine foarte populară. Această abordare a fost adoptată de multe organizații datorită avantajelor sale față de găzduirea tradițională bazată pe server. Site-urile web statice sunt site-uri web care nu necesită niciun mediu de rulare precum JRE, .NET etc. și se bazează în mare parte pe HTML, CSS, JS și alte resurse statice (fișiere audio/video, documente etc.). AWS oferă toate serviciile și instrumentele necesare care vă permit să construiți și să gestionați site-uri web statice pe cloud AWS foarte ușor. Ca în cazul altor găzduiri bazate pe cloud, nu există nicio investiție CAPEX. Cu toate acestea, există un cost operațional neglijabil pentru găzduirea site-ului web static.

Perioada de timp estimată pentru a obține avantaje

1 – 3 luni

3.41 Aplicații de mesagerie instantanee

Scop

Tehnologia de mesagerie instantanee (IM) este un tip de chat online care permite transmiterea textului în timp real prin Internet sau altă rețea de calculatoare. Mesajele sunt transmise de obicei între două sau mai multe părți, atunci când fiecare utilizator introduce text și declanșează o transmisie către destinatarii, care sunt toți conectați la o rețea comună. Diferă de e-mail prin faptul că conversațiile prin mesageria instantanee au loc în timp real (deci „instantaneu”). Cele mai multe aplicații de chat moderne (uneori numite „mesageri sociale”, „aplicații de mesagerie” sau „aplicații de chat”) folosesc tehnologia push și, de asemenea, adaugă alte funcții, cum ar fi emoji-uri (sau emoticone grafice), transfer de fișiere, chatbot , voce peste IP sau video chat.

Scopul aplicațiilor de mesagerie instantanee este de a permite utilizatorilor să trimită și să primească mesaje instantaneu în timp real. Aceste aplicații permit utilizatorilor să comunice între ei, indiferent de locația lor, făcându-le convenabile și eficiente pentru ca oamenii să rămână conectați. Unele dintre obiectivele cheie ale aplicațiilor de mesagerie instant includ:

- Comunicare: Scopul principal al aplicațiilor de mesagerie instantanee este de a oferi utilizatorilor o platformă pentru a comunica între ei în timp real, fie prin mesaje text, apeluri vocale sau apeluri video.
- Comoditate: aplicațiile de mesagerie instantanee sunt concepute pentru a oferi un mijloc de comunicare mai convenabil și mai accesibil decât metodele tradiționale, cum ar fi e-mailul sau apelurile telefonice.
- Conectivitate: Aplicațiile de mesagerie instantanee le permit oamenilor să rămână conectați unul cu altul, în ciuda faptului că se află în locații și fusuri orare diferite.
- Viteză: aplicațiile de mesagerie instantanee sunt concepute pentru a funcționa în timp real, permițând utilizatorilor să trimită și să primească mesaje instantaneu, făcând comunicarea mai rapidă și mai eficientă.
- Confidențialitate: aplicațiile de mesagerie instantanee oferă diverse funcții de confidențialitate, cum ar fi criptarea de la capăt la capăt, pentru a proteja datele și conversațiile utilizatorilor de accesul neautorizat.

În general, scopul aplicațiilor de mesagerie instantanee este de a permite oamenilor să rămână conectați și să comunice între ei rapid, convenabil și în siguranță, indiferent de locul în care se află.

Perioada de timp estimată pentru a obține avantaje

Aplicațiile de mesagerie instantanee pot crea valoare din momentul în care sunt implementate și sunt adoptate pe scară largă de utilizatori. Valoarea pe care o oferă aplicațiile de mesagerie instantanee este capacitatea lor de a conecta oamenii și de a le permite să comunice eficient în timp real. Astfel, cu cât mai mulți oameni folosesc aceste aplicații, cu atât oferă mai multă valoare.

În multe cazuri, aplicațiile de mesagerie instantanee pot crea valoare în câteva minute, de îndată ce utilizatorii încep să folosească platforma pentru a se conecta între ei. De exemplu, un grup de prieteni ar putea descărca o aplicație de mesagerie instantanee, poate crea un chat de grup și poate începe să o folosească pentru a rămâne conectat. În acest scenariu, valoarea este creată aproape imediat.

Într-un cadru de afaceri, aplicațiile de mesagerie instantanee pot dura ceva mai mult pentru a crea valoare, deoarece pot necesita integrarea cu alte sisteme de afaceri, verificarea securității și adoptarea lor de către angajați. Cu toate acestea, odată ce aplicația este implementată complet, poate oferi o valoare semnificativă, permițând angajaților să comunice mai eficient, să colaboreze la proiecte și să răspundă mai rapid clienților.

În general, intervalul de timp așteptat pentru ca o aplicație de mesagerie instantanee să creeze valoare va varia în funcție de situația și contextul în care este implementată. Cu toate acestea, în general, aplicațiile de mesagerie instant pot crea valoare relativ rapid, permițând oamenilor să rămână conectați și să comunice eficient în timp real.

3.42 Gestionarea rețelei virtuale

Scop

Scopul gestionării rețelelor virtuale este de a crea, configura și menține o infrastructură de rețea virtualizată care conectează mașinile virtuale (VM) și alte resurse din cloud.

Perioada de timp estimată pentru a obține avantaje

Timpul necesar pentru a crea valoare din gestionarea rețelelor virtuale depinde de complexitatea rețelei, de numărul de resurse conectate și de obiectivele specifice ale organizației. Cu toate acestea, rețelele virtuale pot oferi beneficii imediate în ceea ce privește îmbunătățirea scalabilității, flexibilității și securității.

3.43 Migrare spre cloud

Scop

Scopul migrării către cloud este de a muta aplicațiile, datele și infrastructura organizației dvs. de la servere locale la o infrastructură bazată pe cloud. Obiectivul este de a creşte agilitatea, de a reduce costurile operaționale, de a spori scalabilitatea și de a îmbunătăți securitatea.

Perioada de timp estimată pentru a obține avantaje

Timpul necesar pentru a crea valoare din migrarea către cloud depinde de mai mulți factori, inclusiv de complexitatea infrastructurii IT existente, domeniul de aplicare al migrării și cantitatea de resurse alocate proiectului. Cu toate acestea, multe organizații văd beneficii semnificative în ceea ce privește creşterea agilității, scalabilitatea și costurile operaționale reduse imediat după migrarea către cloud.

3.44 Monitorizarea activităților desfășurate de mașinile agricole pe o suprafață data

Scop

Munca agricolă efectuată de mașinile conduse de șofer este stresantă și deseori solicită foarte mult șoferul. Aceste lucruri se datorează faptului că operațiuni repetitive sunt efectuate des și uneori în

condiții meteorologice dificile (temperaturi extreme, umiditate ridicată etc.) Șoferul acestor utilaje lucrează uneori în condiții dificile din cauzele prezentate mai sus. Există prea puține posibilități de îmbunătățire a condițiilor de lucru ale șoferului.

Mașinile agricole care funcționează fără a fi conduse direct de oameni par a fi o soluție modernă și viabilă. În acest caz, inteligența artificială și tehnologiile robotice sunt folosite pentru a crește performanța acestor mașini. Aplicația propusă monitorizează activitatea uneia sau mai multor mașini care lucrează pe o suprafață de sol.

Perioada de timp estimată pentru a obține avantaje

1 – 12 luni

3.45 Monitorizarea parametrilor fiziologici ai sportivilor în timpul antrenamentului

Scop

Antrenamentul sportivilor este întotdeauna însoțit de modificări ale valorilor unor parametri fiziologici. Măsurarea acestor parametri și prelucrarea lor ulterioară furnizează date despre modul în care organismul sportivului răspunde la cerințele din timpul antrenamentului.

Depășirea unui anumit nivel poate duce la accidente. Aplicația propune monitorizarea unor parametri fiziologici ai sportivilor în timpul antrenamentului.

Perioada de timp estimată pentru a obține avantaje

3 săptămâni – 4 luni

3.46 Gestionarea mai multor proiecte simultan

Scop

Scopul operării simultane a mai multor proiecte folosind Google Cloud Platform este de a gestiona mai multe proiecte în mod efectiv și eficient, valorificând scalabilitatea, securitatea și rentabilitatea Google Cloud Platform.

Perioada de timp estimată pentru a obține avantaje

Timpul necesar pentru a crea valoare din operarea simultană a mai multor proiecte folosind Google Cloud Platform depinde de complexitatea proiectelor, de numărul de resurse implicate și de obiectivele specifice ale organizației. Cu toate acestea, organizațiile pot vedea beneficii imediate în ceea ce privește îmbunătățirea eficienței, utilizarea resurselor și rezultatele proiectelor.

3.47 Reconfigurarea rutelor de transport public într-un oraş

Scop

Mijloacele de transport în comun dintr-o localitate au un traseu bine delimitat pe care îl parcurg la anumite intervale de timp după un orar stabilit. În orele de vârf, mijloacele de transport în comun sunt mai aglomerate, iar în restul zilei, mijloacele de transport sunt încărcate cu mult sub capacitatea lor nominală (număr de persoane transportate).

Aplicația reconFiguraază traseul de circulație al mijloacelor de transport în comun astfel încât acestea să circule încărcate aproape de capacitatea lor normală și să răspundă cerințelor călătorilor.

Perioada de timp estimată pentru a obţine avantaje

3 luni - 12 luni

3.48 Dispozitive inteligente controlate de la distanţă în casă/birou inteligent

Scop

Acest studiu discută impactul măsurilor de condiții ambientale asupra comportamentului clienților și aplicarea acestuia în industria de retail. Sunt prezentate o structură de bază a seturilor de date care constă din sursele de date respective, și anume senzori IoT, contoare inteligente și baze de date interne tranzacționale și analitice, precum și indicatori de afaceri utilizați pentru optimizarea submediilor de calitate a aerului din magazine. Învățarea automată este propusă pentru a automatiza descoperirea cunoștințelor și descoperirea modelelor din date și punerea bazei unei interfețe cu sistemul de aer condiționat interoperabil.

Perioada de timp estimată pentru a obţine avantaje

6 - 9 luni

3.49 Gestionarea accesului la resurse şi la aplicaţii

Scop

Utilizarea serviciilor IAM pentru a păstra o imagine de ansamblu asupra cine are acces şi la ce resurse și aplicații.

Folosind controlul accesului bazat pe roluri (RBAC) din Azure Active Directory (AD), puteți configura permisiunile pentru utilizatorii dintr-o organizație, definind cine are acces la ce, autentificându-i cu

acreditările Azure AD și apoi autorizându-i prin compararea rolurilor utilizatorul are și permisiunile configurate pentru o anumită aplicație sau resursă. Acest lucru permite stabilirea unei politici cu cel mai mic privilegiu.

Pentru a crește securitatea, implementând diferite moduri de autentificare a utilizatorului, cum ar fi Multi-Factor Authentication (MFA), în care primiți o parolă unică pe dispozitiv, sau biometrie, în care utilizați recunoașterea feței sau amprentele digitale pentru a vă autentifica.

După ce utilizatorul a fost autentificat, serviciul IAM va căuta rolurile utilizatorului, fie că este rolul permanent sau rolul Just-In-Time (JIT) acordat prin Privileged Identity Manager (PIM) și îl va compara cu politica de acces. configurat pe resursa sau aplicația pe care utilizatorul încearcă să o acceseze.

Configurarea identității dispozitivului vă poate de asemenea asigura, că dispozitivul pe care utilizatorul îl folosește în prezent este considerat sigur prin utilizarea accesului condiționat. De asemenea, acesta poate fi configurat pentru a permite accesul numai din anumite locații, cum ar fi într-o anumită locație IP, în anumite intervale de timp sau pentru a utiliza detectarea riscurilor pentru a determina dacă comportamentul utilizatorului este considerat neobișnuit.

Puteți monitoriza utilizarea și acordați autorizație anumitor utilizatori pentru a furniza sau anula conturile resurselor suplimentare. De asemenea, este folosit pentru a vedea ce utilizatori au accesat o anumită resursă sau aplicație la un moment dat, ceea ce poate ajuta la depanarea în cazul în care a avut loc o încălcare a datelor.

Perioada de timp estimată pentru a obține avantaje

3 săptămâni – 1 lună

3.50 Clasificarea site-urilor de phishing pe bază de reguli

Scop

În zilele noastre diverși roboți se târăsc pe internet, care mai sunt numiți: boți, recoltatori (harvesters) sau păianjeni. Motoarele de căutare populare folosesc o tehnică similară pentru a indexa paginile web - au un agent autonom (numit robot sau bot) care este însărcinat cu activitatea de crawling pentru site-urile web. În ultimul timp, această tehnică de crawling este exploatată de utilizatorii rău intenționați, de exemplu recoltatoarele(harvesters), care sunt folosite pentru a răzui adresele de e-mail de pe site-uri web pentru a construi o listă de spam pentru spamboți . Recent, roboții sunt folosiți greșit și pentru a cumpăra bilete de avion sau pentru a face licitații rapide în sistemul de licitații on-line. În această lucrare vă prezentăm un sistem inteligent numit Lino care încearcă să rezolve problema menționată. Lino este un sistem care simulează o pagină web vulnerabilă și captează crawlerele web. Colectăm

diverse caracteristici și efectuăm o procedură de selecție a caracteristicilor pentru a afla care caracteristici contribuie cel mai mult la clasificarea comportamentului vizitatorilor. În scopul clasificării, folosim metode de învățare automată de ultimă generație, cum ar fi Support Vector Machine și arborele de decizie C 4.5.

Perioada de timp estimată pentru a obține avantaje

1 – 3 luni

3.51 SAP Build

Scop

Scopul principal al SAP Build este de a permite utilizatorilor de afaceri și altor părți interesate să creeze ușor și rapid interfețe de utilizator și alte aplicații fără a necesita abilități tehnice. SAP Build este o platformă bazată pe cloud care oferă o interfață drag-and-drop unde utilizatorii pot crea și proiecta cu ușurință aplicații bazate pe web.

Obiectivul principal al SAP Build este de a reduce timpul și efortul necesar pentru proiectarea și dezvoltarea interfețelor utilizator, care este de obicei un proces complex și consumator de timp. Oferă un mediu de colaborare ușor de utilizat, în care utilizatorii de afaceri își pot crea, vizualiza și testa cu ușurință ideile de aplicații fără a necesita asistență din partea dezvoltatorilor tehnici.

SAP Build este conceput pentru a spori experiența generală a utilizatorului și designul interfeței cu utilizatorul a aplicațiilor SAP. Oferă o gamă largă de șabloane, elemente de design și modele care permit utilizatorilor să creeze rapid interfețe intuitive, ușor de utilizat, care sunt în concordanță cu principiile de proiectare SAP.

În general, obiectivul SAP Build este de a da posibilitatea utilizatorilor de afaceri și alte părți interesate să ia parte activă la proiectarea și dezvoltarea interfețelor utilizator, asigurându-se că aplicațiile îndeplinesc nevoile și cerințele lor, respectând în același timp cele mai bune practici în proiectarea și dezvoltarea UI (interfeței utilizator).

Perioada de timp estimată pentru a obține avantaje

Perioada de timp pentru a crea valoare folosind SAP Build depinde de diverși factori, cum ar fi complexitatea interfeței cu utilizatorul, resursele disponibile și nivelul de expertiză al echipei care dezvoltă aplicația. Cu toate acestea, utilizarea SAP Build poate reduce semnificativ timpul și efortul necesar pentru proiectarea și dezvoltarea interfețelor cu utilizatorul, permițând un timp mai scurt de punere pe piață (time-to-market) pentru aplicații.

De obicei, cu SAP Build, utilizatorii pot crea prototipuri interactive și pot efectua testarea utilizatorilor în câteva săptămâni, ceea ce ajută la identificarea din timp a oricăror probleme de proiectare și asigură ca aplicația finală să răspundă nevoilor utilizatorilor.

Utilizarea SAP Build poate îmbunătăți, de asemenea, satisfacția și productivitatea utilizatorilor prin crearea de interfețe mai intuitive și mai ușor de utilizat, rezultând un flux de lucru mai eficient și o experiență mai bună pentru utilizator.

În general, valoarea SAP Build poate fi imediat evidentă, în special prin reducerea timpului și efortului necesar pentru proiectarea și dezvoltarea interfețelor cu utilizatorul, sporind satisfacția și productivitatea utilizatorilor și permițând un timp mai scurt de punere pe piaţă pentru aplicații. Perioada de timp estimată pentru crearea valorii va fi determinată de obiectivele specifice ale organizației și de nevoile de proiectare.

3.52 Configurarea Load Balancers-urilor

Scop

În perioadele de vârf de încărcare, serverele pot primi mai mult trafic decât sunt capabile să gestioneze în mod corespunzător, ceea ce duce la pierderea pachetelor, pierderea de date și laaplicații care nu răspund, ceea ce poate duce din nou la pierderea de utilizatori. Configurarea unui Load Balancer automat va rezolva această problemă prin distribuirea traficului de intrare pe mai multe servere, astfel încât nici un server să nu fie supraîncărcat și să se transforme într-un blocaj. Acest lucru îmbunătățește performanța generală, disponibilitatea și scalabilitatea care se rulează în infrastructura cloud.

Perioada de timp estimată pentru a obţine avantaje

Imediat

3.53 Gestionarea inteligentă a traficului

Scop

Proiectul rezolvă problema nevoii tot mai mari de securitate (mai ales în spațiile publice) și de reglementare a circulației în prezent, direcția în care se dezvoltă zona și care vor fi nevoile în viitorul apropiat. Soluția problemei se va obține prin dezvoltarea unei platforme care, folosind tehnologii avansate de învățare automată, transformă sistemele de monitorizare și control în instrumente care deschid posibilități de aplicare în domeniul traficului inteligent și al securității. Provocările altor sisteme de pe piață sunt văzute prin: (i) o parte a pieţei, există furnizori de soluții care transmit cel mai adesea mesajul că soluțiile lor susțin o abordare cuprinzătoare a supravegherii/securității și

traficului/transportului de cea mai bună practică, cu toate acestea, acele soluții includ doar un număr de bază sau redus de funcționalități și sunt greu/imposibile să susțină interoperabilitatea acelui sistem cu altele pe care le are utilizatorul, astfel de soluții au o orientare accentuată către un anumit (unul) producător, demonstrează tranziție dificilă la alte soluții odată ce soluția specifică este introdusă și, de obicei, sunt costisitoare în ceea ce privește dezvoltarea și introducerea sistemului de bază, precum și orice integrare sau suprastructură (problema de „supra-preț"/„over-promise (a promite mai mult decât este posibil sau realist)"); (ii) pe de altă parte, micile provocări de pe piață prezintă potențial prin utilizarea progreselor tehnologice (suport de circuite și software, adică modele matematice), dar de obicei eşuează in scalarea soluțiilor sau în asigurarea un grad mai mare de cotă de piață din cauza. Costului ridicat pentru dezvoltarea funcționalităților de bază, adică faptul că investiția de bază în dezvoltare pentru a putea oferi chiar și cel mai scăzut nivel de serviciu, de exemplu faptul ca dezvoltarea investitiei de bază ca să poata oferi cel mai scazut nivel de operare are un pret prea mare (problema „abordării de laborator"); (iii) chiar dacă sunt prezentate ca atare, soluțiile de concurență sunt rareori optimizate în domeniul supravegherii/securității și transportului/logisticii cu absența unor modele sau studii clare în care se realizează interoperabilitatea între diferite sisteme și cât mai mulți utilizatori în domeniul supraveghere/securitate și transport/logistică consideră necesar deoarece de-a lungul timpului au investit resurse considerabile în diverse tehnologii; (iv) controlul confidențialității este și o cerință logică, care implică în cea mai mare măsură controlul asupra modelelor care conduc la anumite acțiuni sau stau la baza înțelegerii comportamentului în domeniul supravegherii/securității și transportului/logisticii; (v) în sfârșit, soluțiile din domeniul supravegherii/securității și transportului/logisticii se află adesea sub reglementări legale speciale și sunt supuse unor modificări ale acestora, ceea ce crește necesitatea adaptării lor prin corectarea modelului și construirea unor astfel de sisteme pe tehnologii deschise. cu un grad ridicat de control asupra modelelor care conduc la o mai bună cunoaştere.

Perioada de timp estimată pentru a obține avantaj

12 - 24 luni

3.54 Furnizaţi date de vânzări în timp real

Scop

Pentru a putea folosi informațiile adunate să se facă modificări din zbor la promoții, să se testeze noi promoţii şi să se modifice pe baza feedback-ului continuu sau să se distribuie personalul în mai multe locații pentru a rezolva sarcinile de lucru în perioadele de vârf.

Perioada de timp estimată pentru a obține avantaje

6 luni – 12 luni

3.55 Interfața grafică pentru programare la un service auto combinată cu un site web

Scop

Firmele care oferă servicii populației precum servicii auto, cabinete medicale private, etc își planifică zilnic activitatea, ținând cont de timpul necesar desfășurării unei activități.

De exemplu, dacă mașina unei persoane are o problemă, proprietarul mașinii va trebui să meargă la un atelier pentru a diagnostica mașina, a propune metode de remediere a situației și de a remedia defecțiunea.

Această aplicație oferă clientului posibilitatea de a se programa online la un service auto pentru a diagnostica defecțiunea unei mașini.

Perioada de timp estimată pentru a obține avantaje

2 săptămâni – o lună

3.56 Sistem de videoconferință

Scop

Scopul unui sistem de videoconferință este de a permite comunicarea și colaborarea de la distanță între oameni sau echipe, indiferent de locația lor fizică. În mod specific, obiectivele unui sistem de videoconferință pot include:

- Comunicare în timp real: un sistem de videoconferință își propune să ofere o platformă pentru interacțiunea față în față în timp real între participanți, permițând echipelor sau indivizilor la distanță să comunice în mod natural și eficient.
- Colaborare: Un sistem de videoconferință poate facilita colaborarea, permițând participanților să partajeze fișiere, documente și ecrane, să elaboreze documente și chiar să facă brainstorming pe table virtuale.
- Comoditate: Un sistem de videoconferință își propune să ofere confort și flexibilitate, eliminând necesitatea ca participanții să fie prezenți fizic în aceeași locație, permițându-le să participe la întâlniri de oriunde în lume.
- Economie de timp: un sistem de videoconferință poate ajuta la economisirea timpului evitând nevoia de deplasare și reducând timpul de nefuncționare dintre întâlniri, permițând participanților să rămână productivi și implicați.
- Economii de costuri: Un sistem de videoconferință poate ajuta la economisirea costurilor asociate cu călătoria și cazarea, în special pentru organizațiile cu mai multe birouri în diferite

locații sau pentru echipele aflate la distanță care altfel ar avea nevoie de spațiu de birou pentru a funcționa.

În general, un sistem de videoconferință își propune să ofere o modalitate simplă și eficientă de a comunica și de a colabora de la distanță pentru echipe sau indivizi, sporind productivitatea, confortul și economiile de costuri.

Perioada de timp estimată pentru a obține avantaje

Perioada de timp estimată pentru a crea valoare dintr-un sistem de videoconferință depinde de diverși factori, cum ar fi mărimea organizației, structura operațională a acesteia, frecvența întâlnirilor și ecosistemul tehnologic. Iată câteva exemple generale:

- Colaborare îmbunătățită: sistemele de videoconferință pot îmbunătăți colaborarea oferind capabilități video și audio în timp real, facilitând colaborarea echipelor de la distanță. Valoarea acestei caracteristici poate fi realizată pe termen scurt, chiar și în timpul primelor videoconferințe.
- Cheltuieli reduse de călătorie: sistemele de videoconferință pot economisi costurile de călătorie prin înlocuirea întâlnirilor în persoană cu cele virtuale, ceea ce duce la reducerea cheltuielilor de călătorie, cum ar fi zborurile, cazarea și transportul. Valoarea din cheltuielile reduse de călătorie poate fi realizată imediat, în timpul primelor videoconferințe sau întâlniri în care se evită călătoriile.
- Luare mai rapidă a deciziilor: sistemele de videoconferință pot facilita luarea mai rapidă a deciziilor, oferind acces instantaneu la video și audio, susținând luarea deciziilor în timp real. Valoarea unei decizii mai rapide poate fi realizată imediat și pe parcursul utilizării pe termen lung a sistemului.

În general, intervalul de timp estimat pentru a crea valoare dintr-un sistem de videoconferință poate fi imediat, în special în ceea ce privește economiile de costuri prin reducerea cheltuielilor de călătorie și îmbunătățirea colaborării. Valoarea suplimentară se poate materializa pe termen mediu și lung, deoarece organizația dezvoltă un ecosistem stabil cu procese și tehnologie bine construite pentru a sprijini întâlnirile și colaborările.

3.57 Oferta VoD

Scop

Cu Video la cerere (Video on Demand (VoD)), puteți crea o bibliotecă de videoclipuri pe care utilizatorii dvs. o pot accesa în orice moment. De asemenea, puteți controla accesul la videoclipurile dvs.

specificând cine le poate vizualiza și când. AMS oferă, de asemenea, instrumente care vă ajută să vă gestionați conținutul video, inclusiv indexare, căutare și analiză.

Pentru a utiliza Azure Media Service (AMS) VoD , mai întâi trebuie să vă încărcați videoclipurile pe platformă. Puteți face acest lucru prin portalul AMS, API-urile REST sau printr-o varietate de instrumente și servicii terțe. Odată ce videoclipurile dvs. sunt încărcate, puteți utiliza AMS pentru a le transcoda în diferite formate, pentru a crea mai multe rate de biți și pentru a le cripta pentru livrare sigură.

După ce videoclipurile dvs. sunt procesate, puteți utiliza playerul AMS pentru a le încorpora pe site-ul sau în aplicația dvs. Playerul acceptă o varietate de funcții, inclusiv streaming adaptiv, subtitrări închise și mai multe piese audio. De asemenea, puteți personaliza aspectul și senzația jucătorului pentru a se potrivi cu marca dvs.

Perioada de timp estimată pentru a obține avantaje

2 luni – 4 luni

3.58 Gestionarea alimentării cu apă folosind cititoare la distanță în rețelele de alimentare cu apă

Scop

Transformarea digitală permite economii semnificative prin gestionarea resurselor și îmbunătățirea proceselor de afaceri. Schimbă modul în care folosim informațiile pe care le avem, tipul și cantitatea de date pe care le putem colecta. Pentru a face aceste date mai utilizabile, folosim instrumente moderne de analiză și vizualizare a căror sarcină este de a obține informații utile și timp util dintr-o cantitate mare de date diferite într-un mod simplu și flexibil.

Problemele care apar în acest domeniu de interes variază de la modul de vizualizare a datelor, ce metode să folosească pentru a găsi cunoștințe ascunse în date și cum se dezvoltă modele de prognoză folosind date.

Cercetătorii și industria acordă o atenție specială datelor meteorologice care pot avea un impact semnificativ asupra predicției în vremuri de schimbări climatice imprevizibile și influențe meteorologice. În materie tehnică pentru companiile care doresc să facă primul pas în acest domeniu, acestea se confruntă cu întrebări legate de modul de stocare a datelor într-un container „cloud”/„big data”, este posibil să se dezvolte un proiect de date care „crește împreună cu o companie” și din ce în ce mai multe date dobândite, fie că toate pot funcționa în timp real și este acest „pachet” la dispoziție în ceea ce privește costul și cunoștințele necesare.

Perioada de timp estimată pentru a obține avantaje
6 – 9 luni

3.59 Aplicație web pentru completarea online a fișei de pontaj a personalului unei companii

Scop
Firmele de construcții desfășoară lucrări în diferite puncte de lucru situate într-un spațiu geografic. La fiecare lucrare participă echipe detașate pe toată durata lucrării.

La sediul firmei trebuie ținută evidența orelor lucrate de fiecare membru al echipei de lucru. Aplicația permite ca prezența să fie completată la zi pentru fiecare membru al echipelor care își desfășoară activitatea în diferite puncte de lucru.

Perioada de timp estimată pentru a obține avantaje
3 săptămâni - 1 lună

3.60 Găzduire site cu conținut static

Scop
A avea un site web este crucial pentru ca orice afacere de astăzi să rămână competitivă. Oferă companiei oportunitatea de a menține o prezență online pentru viitori clienți și utilizatori, oferind companiei disponibilitate 24/7, vizibilitate și accesibilitate pentru actuali și potențiali noi utilizatori. Acest lucru le oferă posibilitatea de a vă descoperi afacerea fără a fi restricționați de lucruri precum programul de deschidere, timpii de așteptare la telefon și trebuința de a vizita o locație fizică.

Chiar și cele mai simple site-uri web vor permite afacerii să ofere informații vizitatorilor despre lucruri precum programul de deschidere al unei anumite locații, informații de contact sau informații despre produsele sau serviciile pe care compania le oferă. Poate fi folosit și pentru a afișa videoclipuri și fotografii care promovează afacerea și produsele/serviciile acesteia.

Acest lucru înseamnă că a avea un site web ar putea oferi unei afaceri o accesibilitate și o prezență la nivel global, reducând în același timp timpul și costurile cheltuite cu serviciul/asistența clienților, având răspuns la multe întrebări frecvente pe site. Și oferă o platformă convenabilă pentru interacțiunea cu clienții/utilizatorii prin afișarea de produse și servicii prin intermediul materialelor promoționale, cum ar fi videoclipuri găzduite pe site-ul web sau trimiterea de buletine informative cu oferte exclusive sau reduceri trimise direct clienților/utilizatorilor interesați către un public global.

Perioada de timp estimată pentru a obține avantaje

1 săptămână – 6 luni

3.61 Magazin online

Scop

Vânzarea produselor, fie online, fie într-o locație fizică sau în ambele, având acces la informații precise și concomitente despre starea actuală a inventarului de produse este important pentru a putea oferi cea mai bună experiență posibilă pentru un client și pentru a minimiza riscul epuizării stocului care poate duce la întârzieri de comenzi și clienți nemulțumiți.

Păstrarea evidenței clienților și a comenzilor pe care le-au făcut este, de asemenea, importantă, atât pentru a vă asigura că puteți oferi un nivel adecvat de asistență pentru client adresat clientului dvs., cât și pentru a obține o perspectivă importantă asupra comportamentului clientului dvs., cum ar fi tipul de produse care îi interesează care pot fi folosite pentru a crea conținut personalizat pentru clienții dvs.

Perioada de timp estimată pentru a obține avantaje

2 săptămâni – 2 luni

LITERATURE

1. Cloud Industry Forum. (2022). *8 criteria to ensure you select the right cloud service provider.* Retrieved from https://cloudindustryforum.org/8-criteria-to-ensure-you-select-the-right-cloud-service-provider/
2. CloudSigma. (2023). *10 Steps to Choose the Best Cloud Provider.* Retrieved from https://www.cloudsigma.com/10-steps-to-choose-the-best-cloud-provider/
3. Colt. (2023). *Cloud connect explained.* Retrieved from https://www.colt.net/resources/cloud-connect-explained/
4. CompTIA. (2022). *A cloud networking quick-start guide: around the network in 8 steps.* Retrieved from https://www.comptia.org/content/guides/cloud-network-setup-guide
5. CompTIA. (2023). *Partly Cloudy with a Chance of Computing: A Beginner's Guide to Cloud Types, Solutions and Vendors.* Retrieved from https://www.comptia.org/content/articles/cloud-types-solutions-and-vendors
6. CompTIA. (n. a.). *Partly Cloudy with a Chance of Computing: A Beginner's Guide to Cloud Types, Solutions and Vendors.* Retrieved from https://www.comptia.org/content/articles/cloud-types-solutions-and-vendors
7. Delta. (2020). *Powering Competitiveness in Datacentres.* Retrieved from https://www.deltapowersolutions.com/en/mcis/technical-article-powering-competitiveness-in-datacenters.php
8. Dialogic. (2017). *Introduction to Cloud Computing, White paper.* Retrieved from https://www.dialogic.com/~/media/products/docs/whitepapers/12023-cloud-computing-wp.pdf
9. Dialogic. (2017). Introduction to Cloud Computing, White paper. Retrieved from https://www.dialogic.com/~/media/products/docs/whitepapers/12023-cloud-computing-wp.pdf
10. Eldh, E. (2013). *Cloud connectivity for embedded systems (Master of Science Thesis).* KTH Royal Institute of Technology, Stockholm, Sweden.
11. Faddom. (2021). Cloud Computing Costs & Pricing Comparisons for 2023. Retrieved from https://faddom.com/cloud-computing-costs-and-pricing-comparison/
12. FERI. (2022). *Cloud Calculation.* Retrieved from: https://moja.um.si/studijski-programi/Strani/ucnaenota.aspx?jezik=S&fakulteta=FERI&sifraue=61M252
13. FRI. (2022). *Second Level Master's Study Program Computing and Informatics Presentation Proceedings for Students First Enrolled in The 1st Year In The Academic Year 2022/2023 Ljubljana*. Retrieved from: 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 documentation.* Retrieved from https://cloud.google.com/network-connectivity/docs/interconnect
15. Google Cloud. (2022b). *Google Cloud terms.* Retrieved from https://cloud.google.com/network-connectivity/docs/concepts/key-terms
16. ITPro Today. (2022a). 2022 *Cloud Computing Trends.* Retrieved from https://www.youtube.com/watch?v=PiaouNqFNwA
17. ITRPro Today. (2022b). *Providers Continue to Dominate, Led by AWS.* Retrieved from https://www.itprotoday.com/iaas-and-paas/big-3-public-cloud-providers-continue-dominate-led-aws#close-modal
18. ITU. (2012). *Technical Report: Part 1: Introduction to the cloud ecosystem: definitions, taxonomies, use cases and high-level requirements.* Retrieved from https://www.itu.int/pub/T-FG-CLOUD-2012-P1
19. ITU. (2022). *Focus Group Cloud, Technical Report, Part 1: Introduction to the cloud ecosystem: definitions, taxonomies, use cases and high-level requirements, Version 1.0*. Retrieved from https://www.itu.int/pub/T-FG-CLOUD-2012-P1
20. Jones, E. (2022). *Cloud Market Share: A Look at the Cloud Ecosystem in 2023*. Retrieved from https://kinsta.com/blog/cloud-market-share/
21. Letica, J. & Buić, N. (2014). *Innovation in VET.* Retrieved from http://www.refernet.hr/media/1236/innovation-in-vet_croatia.pdf
22. Marinescu, D. (2017). *Cloud computing Theory and Practice*. USA: Elsevier, Morgan Kaufmann publishing.
23. Markets And Markets. (2019). Retrieved from https://www.marketsandmarkets.com/
24. Marko, K. (2021). *Cloud providers jockey for 2021 market share.* Retrieved from https://www.techtarget.com/searchcloudcomputing/opinion/Cloud-providers-jockey-for-market-share
25. Opinion of the European Economic and Social Committee on 'Industry 4.0 and digital transformation: where to go'. (2016). Retrieved from: 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. Oracle (2023). *What is could computing?* Retrieved from https://www.oracle.com/cloud/what-is-cloud-computing/top-10-benefits-cloud-computing/
27. Peterson, R. (2023). *Cloud Computing Tutorial for Beginners: What is & Architecture.* Retrieved from https://www.guru99.com/cloud-computing-for-beginners.html

28. Rathore, A. (2022). *How To Find The Best Cloud Server For Small Businesses?* Retrieved from https://kanakinfosystems.com/blog/best-cloud-server-for-small-business
29. Resonate. (2020). *What Are the Different Types of Load Balancers?* Retrieved from https://www.resonatenetworks.com/2020/05/25/what-are-the-different-types-of-load-balancers/
30. Richter, F. (2023). *Big Three Dominate the Global Cloud Market.* Retrieved from https://www.statista.com/chart/18819/worldwide-market-share-of-leading-cloud-infrastructure-service-providers/
31. Rosencrance, L. (2021). *Breaking Down the Cost of Cloud Computing in 2023.* Retrieved from https://www.techtarget.com/whatis/Breaking-Down-the-Cost-of-Cloud-Computing
32. Samoshki, D. (n. d.). *The cloud report.* Retrieved from https://the-report.cloud/how-to-choose-a-cloud-for-your-business/
33. Sharma, M. (2023). *Load balancing in Cloud Computing.* Retrieved from https://www.geeksforgeeks.org/load-balancing-in-cloud-computing/
34. Sharwood, S. (2022). *Cloud a three-player market dominated by AWS, Google, Microsoft.* Retrieved rom https://www.theregister.com/2022/05/02/cloud_market_share_q1_2022/
35. Slovenska strategija pametne specializacije S4. (2017). Retrieved from: chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/viewer.html?pdfurl=https%3A%2F%2Fwww.gov.si%2Fassets%2Fvladne-sluzbe%2FSVRK%2FS4-Slovenska-strategija-pametne-specializacije%2FSlovenska-strategija-pametne-specializacije.pdf&clen=1536948.
36. Spaanenburg, L. & Spaanenburg, H. (2010). *Cloud Connectivity and Embedded Sensory Systems*. New York: Springer.
37. Spaanenburg, L., Spaanenburg, H. (2010). *Cloud Connectivity and Embedded Sensory Systems.* Switzerland: Springer.
38. Spilka, S. (2021). *Cloud Pricing Models - Shedding light upon pricing options.* Retrieved from https://www.exoscale.com/syslog/cloud-pricing-models/
39. Strategija dolgožive družbe. (2017). Retrieved from: chrome-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. Strategija razvoja Slovenije 2030. (2017). Retrieved from: chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/viewer.html?pdfurl=https%3A%2F%2Fwww.gov.si%2Fassets%2Fvladne-sluzbe%2FSVRK%2FStrategija-razvoja-Slovenije-2030%2FStrategija_razvoja_Slovenije_2030.pdf&clen=4124906.
41. Strategija višjega strokovnega izobraževanja v Republiki Sloveniji za obdobje 2020-2030. (2017). Retrieved from: chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/viewer.html?pdfurl=https%3A%2F%2Fwww.gov.si%2Fassets%2Fministrstva%2FMIZS%2FDokumenti%2FVisje-strokovno-

izobrazevanje%2FStrategija-visjega-strokovnega-izobrazevanje-RS-2020-2030%2FStrategija-visjega-strokovnega-izobrazevanja-v-Republiki-Sloveniji-za-obdobje-20202030.pdf&clen=1259647.

42. Suhag, A. (2020). *What Are The Different Types Of Cloud Load Balancing?* Retrieved from https://www.cloudmanagementinsider.com/different-types-of-cloud-load-balancing/
43. Techfunnel. (2021). 14 Incredible Benefits of Cloud Computing for Businesses. Retrieved from https://www.techfunnel.com/information-technology/benefits-of-cloud-computing/
44. The Complete Cloud Computing Manual. (2022). Retrieved from https://online.fliphtml5.com/dslwu/jeti/
45. Tripney S. & Hombrados J. (2013). Technical and vocational education and training (TVET) for young people in low- and middle-income countries: a systematic review and meta-analysis. *Journal of Empirical Research in Vocational Education and Training, 5*(3), 1-14. doi: 10.1186/1877-6345-5-3.
46. Velte, A. T., Velte, J. V., & Elsenpeter, R. (2010). *Cloud Computing: A Practical Approach.* New York: The McGraw-Hill.
47. Westlake. (2022). *Benefits of cloud computing for businesses.* Retrieved from https://www.westlake-it.co.uk/news/2022/05/30/benefits-of-cloud-computing-for-businesses/
48. Wikipedia. (2022). *Border Gateway Protocol.* Retrieved from https://en.wikipedia.org/wiki/Border_Gateway_Protocol
49. Wired. (2020). *Data Centers Aren't Devouring the Planet's Electricity—Yet.* Retrieved from https://www.wired.com/story/data-centers-not-devouring-planet-electricity-yet/

APENDICE

Apendice 1: Cazul campaniei prezidențiale din SUA din 2012 și modul în care AWS l-a sprijinit pe Obama

În această unitate, vom privi la modul în care tehnologia cloud computing a Amazon a permis campaniei prezidențiale din 2012 a președintelui Obama să evite o investiție în IT care ar fi ajuns la zeci de milioane de dolari.

O privire asupra studiului nostru de caz:
Echipa IT a campaniei a folosit AWS pentru a-şi construi, lansa, rula și dezvolta aplicațiile. Urmărind alegerile, au înregistrat totul pe Amazon S3 și au scalat mult, foarte jos. Ei au creat și operat peste 200 de aplicații AWS care pot manipula milioane de oameni. În ultimele patru zile ale campaniei, una dintre aceste aplicații, instrumentul de apel pentru campanie, a manipulat 7.000 de utilizatori concurenți și a efectuat peste două milioane de apeluri.

De ce să folosiți AWS?
Iată trei aspecte cheie care au influențat de ce AWS a fost folosit ca furnizor de cloud computing în campania Obama:

1. Securitate și conformitate

Alegerile atrag unele dintre cele mai agresive amenințări la adresa securității informațiilor din lume. Când vine vorba de tehnologia electorală, securitatea informațiilor este o prioritate majoră. AWS înțelege responsabilitățile administratorilor electorali și îndeplinește sau depășește standardele de securitate și conformitate la fiecare nivel al călătoriei în cloud a clienților noștri. AWS acordă prioritate securității datelor, iar infrastructura lor mondială este dezvoltată și gestionată în conformitate cu cele mai bune practici de securitate.

2. Implicarea votanţilor

În 2018, toți milenialii (cei cu vârsta cuprinsă între 18 și 29 de ani) au fost eligibili să voteze în Statele Unite pentru prima dată. Milenialii preferă tranzacțiile online și au așteptări mari în privinţa experiențelor personalizate pentru clienți. AWS a oferit blocuri constructive care pot fi asamblate rapid pentru a suporta practic orice sarcină de lucru sigură pentru o popularizare țintită.

3. Managementul alegerilor:

Managementul alegerilor se referă la sarcinile de back-office, cum ar fi înregistrarea alegătorilor, care servesc ca factori de eficiență operațională în mai multe sisteme, aplicații și organizații locale conectate din județe și districte. AWS oferă o serie de servicii de baze de date pentru a ajuta la înregistrarea alegătorilor. Aceste sisteme complet gestionate pot fi lansate în câteva minute cu câteva clicuri. Mai mult decât atât, serviciul de migrare a bazelor de date AWS facilitează o tranziție simplă și rentabilă la AWS Cloud.

Cum s-a făcut:

- Registrul principal al informațiilor din fișierul votanţilor a fost o bază de date găzduită pe Amazon RDS. Această bază de date a combinat date din diverse surse (inclusiv www.barackobama.com și informații despre donatori de la echipa financiară) pentru a oferi managerilor de campanie o imagine dinamică, complet integrată a ceea ce se întâmplă.
- Această colecție de baze de date le-a permis lucrătorilor din campanie să vizeze și să segmenteze potențialii alegători, să schimbe resursele de marketing pe baza feedbackului aproape în timp real privind eficacitatea anumitor anunțuri și să alimenteze un sistem de donații care a strâns peste 1 miliard USD (al 30-lea cel mai mare site de comerț electronic din lume).

Aplicațiile campaniei Obama sunt echivalente ca amploare și complexitate cu cele văzute în cele mai mari companii și startup-uri bogate în date.

Pentru a oferi un exemplu punct cu punct al modului în care campania electorală a folosit aplicațiile care erau disponibile pe platforma cloud AWS și a îndeplinit sarcini atât complexe, cât și masive la scară:

- Vertica și Elastic MapReduce sunt folosite pentru a modela cantități masive de date.
- Gestionarea media multicanal prin TV, tipărire, online, mobil, radio și e-mail cu producție dinamică, direcționare, retargeting și testare cu mai multe variante, similar cu ceea ce ați găsi într-o agenție media digitală competentă.
- Coordonarea și colaborarea voluntarilor, contribuitorilor și susținătorilor la nivel social.
- Procesarea tranzacțiilor la scară largă.
- Prevenirea și protecția abuzului alegătorilor, inclusiv colectarea incidentelor și desfășurarea voluntarilor.
- Un sistem cuprinzător de distribuție a informațiilor pentru știri despre campanie, sondaje, informații despre subiecte, înregistrarea alegătorilor și multe altele.
-

De la alegerile prezidențiale din SUA din 2016, Amazon Web Services și-a mărit în liniște prezența la alegerile statale și locale; peste 40 de state folosesc acum una sau mai multe dintre ofertele electorale ale Amazon, la fel ca cele două partide politice majore ale Americii, candidatul democrat la președinție Joe Biden și agenția federală însărcinată cu aplicarea legilor federale privind finanțarea campaniei.

Deși nu se ocupă de votul în ziua alegerilor, conform documentelor și interviurilor companiei, AWS gestionează acum site-uri web privind alegerile de stat și județene, stochează listele de înregistrare a alegătorilor și datele din buletinul de vot, facilitează votul din străinătate de către personalul militar și ajută la furnizarea de rezultate directe în noaptea alegerilor.

Cu toate acestea, prezența în creștere a Amazon în industria electorală poate periclita ceea ce mulți oficiali consideră un punct forte al sistemului de vot din SUA: descentralizarea.

În timp ce majoritatea experților în securitate sunt de acord că, deși cloud-ul Amazon este probabil mult mai dificil de piratat decât sistemele pe care le înlocuiește, punerea datelor din mai multe jurisdicții pe un singur sistem ridică posibilitatea ca o singură breșă majoră să fie dezastruoasă. „Face din Amazon o țintă mai atractivă pentru hackeri" și „crește dificultatea de a face față unui atac din interior", a declarat Chris Vickery, director de cercetare a riscurilor cibernetice la startup-ul de securitate cibernetică Upguard.

Privatizarea infrastructurii de votare face parte dintr-o tendință mai largă care a cuprins aproape toate aspectele guvernamentale din America, de la bilete de parcare până la închisori, și continuă sub administrația Trump.

Potrivit companiilor care au parteneriat cu ambele firme pentru contracte guvernamentale, Azure, principalul concurent al AWS, are o afacere guvernamentală considerabilă și oferă unele servicii electorale, dar nu s-a concentrat asupra acestora și rămâne în urma Amazon.

Întrebări de luat în considerare:
1. Care sunt avantajele plasării alegerilor pe o platformă cloud?
2.Cum este considerată descentralizarea o amenințare?
3. Citiți și comentați despre modul în care AWS a folosit analiza sentimentelor pentru a reflecta asupra discursurilor de inaugurare ale lui Obama vs Trump și asupra concluziilor făcute:
https://medium.com/@szekelygergoo/use-aws-to-compare-inauguration-speeches-of-obama-and-trump-670068ea39d5

Apendice 2: Fragmente de cod

Caz de utilizare : Chatbot pentru studenții din instituția EDU

Importanța înțelegerii limbajului natural (NLU) nu poate fi evidențiată suficient, dar acesta este principalul motiv pentru care această teză se gândește chiar să fie înscrisă. Din perspectiva tehnologiei, Microsoft are servicii foarte bune de oferit. Language Understanding Service (LUIS) este una dintre cele mai bune soluții NLU de pe piață. Cu toate acestea, fiecare serviciu Microsoft care este cumva în relație cu NLU este cuplat la LUIS în fundal. Cu LUIS este ușor să adăugați înțelegere a limbii oricărei aplicații. Este conceput pentru a identifica informații valoroase în conversații, LUIS interpretează scopurile utilizatorului (intențiile) și distileaza informații valoroase din propoziții (entități), pentru un model de limbaj de înaltă calitate, nuanțat. LUIS se integrează perfect cu Azure Bot Service, facilitând crearea unui bot sofisticat.

```
{
   "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
       }
   ]
}
```


Figura 0.1. LUIS in Actiune

De exemplu, pentru o interogare precum „Rezervați-mi un zbor către Cario ”, LUIS este capabil să transforme rezultatele într-un formular JSON. unde ar putea fi găsite informații valoroase precum BookFlight ca intenție cu 98% de acuratețe și entități precum Cairo ca entitate de locație cu 95% de acuratețe. Chiar dacă Boții și NLU sunt tehnologii destul de mature, există încă posibilități ca unele întrebări ale studenților să rămână fără răspuns sau să fie înțelese greșit. Aceste situații ar trebui să fie bine tratate, iar studenții ar trebui să aibă o altă opțiune posibilă pentru a-și îndeplini cererea. Una dintre abordările comune pentru această situație sunt răspunsurile rapide. Răspunsurile rapide sunt butoane sau meniuri mici care au pregătit deja și au prezis posibile întrebări care pot fi scrise dar și alese selectând întrebarea potrivită.

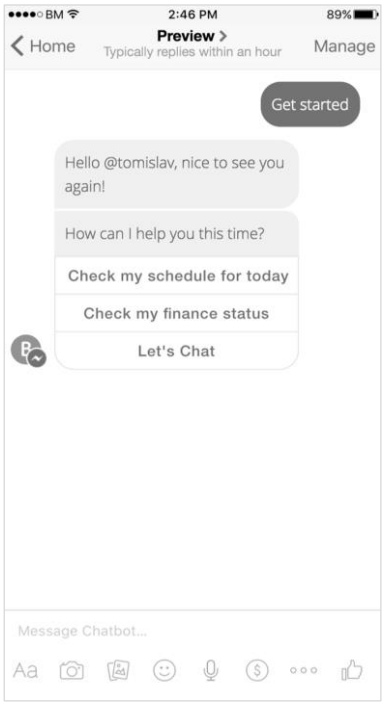

Figura 0.2. Răspunsuri rapide

O altă soluție posibilă este să oferiți posibilitatea să discutați sau să apelați direct personalul de la Biroul Studenților, dar asta ar trebui să fie doar în ultimul caz. Ideea principală a Chatbot-ului de asistență pentru studenți este de a reduce numărul de apeluri ale studenților la minim.

Caz de utilizare: Certificarea activelor digitale folosind registru distribuit/ blockchain

Module de aplicație

Acest tip de aplicație este menită blockchainului privat . Aceasta înseamnă că fiecare instituție de învățământ ar trebui să aibă propriul flux pe care numai oamenii din instituție au autoritatea de a stoca diploma. Toate fluxurile sunt stocate în cartea principală care este distribuită tuturor nodurilor, adică instituțiilor de învățământ în acest exemplu. Cu cât sunt mai multe noduri în lanț, cu atât mai bine, deoarece lanțul devine din ce în ce mai puternic și mai sigur.

Aplicația constă din trei module:

1. Modulul pentru introducerea unei diplome
2. Modulul de verificare a diplomei
3. Modulul de imprimare a diplomelor

Primul modul este pentru introducerea unei diplome. Schimbă datele introduse într-o formă hexazecimală și le stochează în lanț și returnează înapoi ID-ul tranzacției (txid). ID-ul tranzacției este o cheie privată care este acordată unui student absolvent, deoarece poate fi folosită pentru a verifica datele diplomei din lanț. Modulul de verificare a diplomei, combinat cu OIB și ID-ul tranzacției, trimite

o interogare la lanț și verifică dacă există o înregistrare în lanț. După aceea, dă un răspuns pozitiv sau negativ, în funcție de faptul dacă există o diplomă cu adevărat cerută în lanț și dacă respectă OIB-ul introdus. Modulul de imprimare a diplomelor imprimă o diplomă pe ecran în format PDF. Toate modulele enumerate în acest exemplu sunt afișate în interfața text din linia de comandă, adică în terminalul sistemului de operare Ubuntu. Ele pot fi, de asemenea, programate într-o aplicație web și utilizate în browserele WEB.

Roluri de utilizator

După ce studentul finalizează cu succes facultatea și își susține teza de licență, sistemul facultății raportează că studentul a absolvit. Cu această aplicație și cu modulul de introducere a diplomei, o persoană autorizată la universitate va introduce numele, prenumele și absolventul OIB și aceste informații vor fi stocate în lanț. Ca feedback, el primește un ID de tranzacție pe care îl oferă studentului și se înscrie pe diploma originală tipărită. Poate fi tipărit și sub forma unui cod de bare a cărui scanare este valoarea ID-ului Tranzacției.

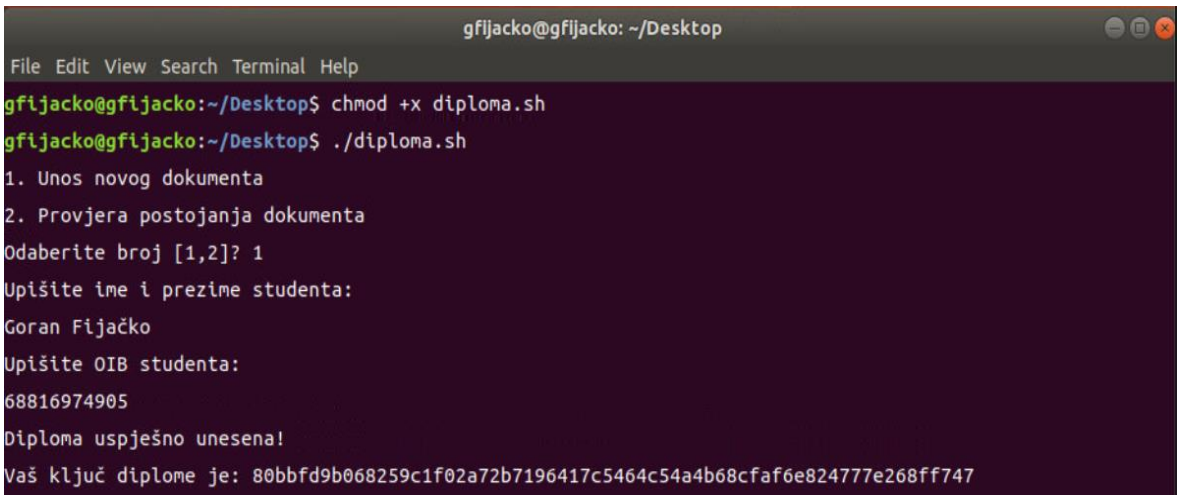

Figura 0.3. Modulul pentru introducerea diplomei

Studentul primește diploma meritată și diploma cu cheie privată, care în acest caz este 80bbfd9b068259c1f02a72b7196417c5464c54a4b68cfaf6e824777e268ff747. Apoi se prezinta la un loc de munca si după un apel de la angajator merge la interviul de angajare. Angajatorul cere o diplomă pentru a-și verifica calificările. Procedura se desfășoară în prezent astfel încât angajatorul să contacteze instituția de învățământ pentru a verifica valabilitatea diplomei, cel mai adesea în scris. Acest proces este de lungă durată și consumă multe resurse. Dar în acest caz, angajatorul primește o diplomă cu cheie privată. Apoi, angajatorul stabileşte OIB-ul persoanei care aplică pentru un loc de muncă cu cheia publică din cerere. Astfel, într-o fracțiune de secundă, se returnează informațiile despre valabilitatea diplomei.

Figura 0.4. Modulul de verificare a diplomei

După ce se răspunde la confirmarea aplicației, ecranul imprimă. Numele și prenumele studentului, instituția de învățământ, orientarea, data și locul absolvirii sunt scrise în imprimare. Angajatorul are eventual opțiunea de a tipări o copie a diplomei pentru propria arhivă. Dacă alegeți o opțiune de tipărire, diploma va fi generată și deschisă în format PDF.

Pentru ușurința utilizării aplicației după lansarea în producție, este o alegere mai bună să o utilizați ca aplicație WEB. Aceasta înseamnă că tot ceea ce este afișat va fi mutat pe un server web și aplicația va accesa protocolul https (de exemplu, prin URL https://www.diplome.hr) în browserele web. Aceasta înseamnă că utilizatorii au nevoie doar de o conexiune la internet și de un cont în aplicație pentru a verifica rapid și în siguranță valabilitatea diplomei.

Caz de utilizare : Dispozitive inteligente controlate de la distanță în casa inteligentă

Pentru a interpreta efectul condițiilor ambientale ale magazinelor asupra comportamentului clienților, putem folosi senzori IoT pentru a măsura luminozitatea, temperatura și umiditatea și pentru a determina/controla influența acestora asupra coșului clienților. Aceasta implică determinarea pragurilor pentru luminozitate nefavorabilă , temperatură neplăcută și niveluri inadecvate de umiditate. Soluția tehnologică ar trebui implementată sub forma unui sistem de suport decizional care poate analiza relațiile reciproce dintre datele colectate IoT , grupurile specifice de produse și tranzacțiile generale din magazin. O parte a sistemului de sprijinire a deciziilor ar trebui să poată controla condițiile tehnice într-o manieră automată prin interfața interoperabilă încorporată în sistemele de aer condiționat existente. Deoarece condițiile de mediu nu sunt de obicei egale în întregul magazin, deoarece unele produse pot necesita condiții diferite (de exemplu, alimentele congelate au un interval

de temperatură ambientală acceptabil diferit față de alte alimente), ar trebui să includem în seturile de date analitice zona de magazin care identifică o anumită arie care necesită condiţii specifice de mediu. Punctele de date propuse sunt împărțite în două niveluri de granularitate: vizita la magazin și produsul cumpărat. Punctele de date sunt colectate din bazele de date tranzacționale existente și din depozitul de date care conține date în timp real ale senzorilor IoT.

Tabelele surselor de date tranzacționale sunt după cum urmează în Figura 5.5:

Environment

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

Transactions

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

Products

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

Visits

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

Figura 0.5. Sursa pentru datele transnaţionale

In figura de mai jos (Figura 5.6.) sunt arătate relatiile ETL:

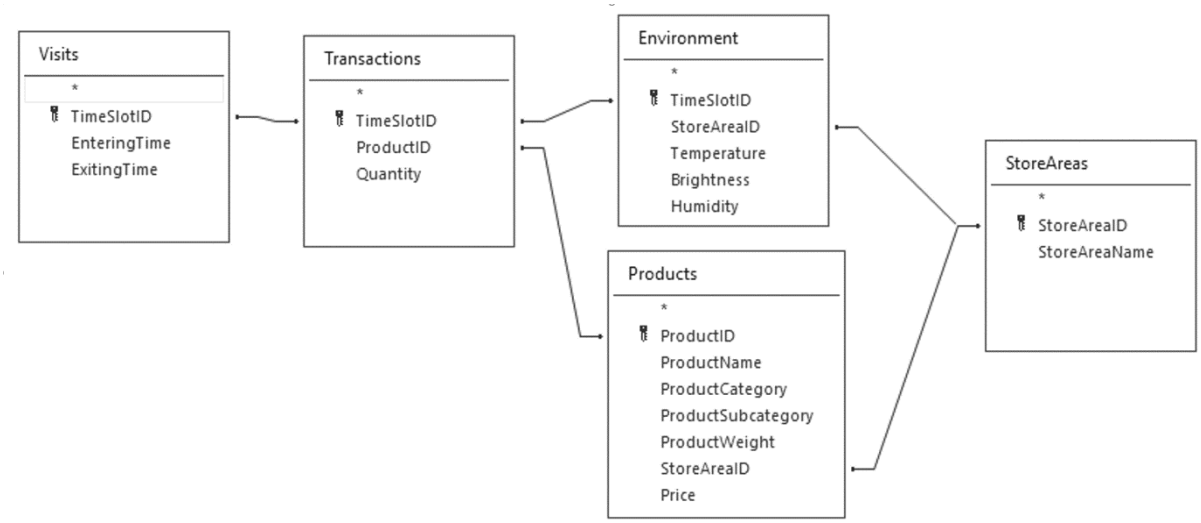

Figura 0.6. Relatiile ETL

Variabilele disponibile pentru analiza vizitelor la magazin după aplicarea procedurii ETL sunt (Figura 5.7.):

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	

Figura 0.7. Variabilele după aplicarea procedurii ETL

Ca variabile țintă pentru învățarea automată, acum putem deriva:

- Număr de articole (N) – numărul de produse diferite achiziționate de un client într-o vizită la magazin (adică numărul de articole din coșul de cumpărături);
- Greutatea achizițiilor (W) – greutatea tuturor produselor achiziționate de un client într-o singură vizită la magazin
- Cantitatea de articole (Q) – cantitatea de articole din toate produsele (însumată pentru toate tipurile de produse) achiziționate de un client într-o singură vizită la magazin.

Alt grupe de variabile țintă posibile – indicatori de afaceri cu amănuntul – sunt descrise separat în secțiunea următoare.

Caz de utilizare : Automatizarea sarcinilor folosind servicii bazate pe cloud

Pentru a demonstra cum se realizează un MBA a fost folosit limbajul de programare R și, în special, pachetul arules, împreună cu un cod inclus ca dovadă de concept. Exemplul folosit este disponibil la arulesViz Vignette și utilizează un set de date despre vânzările de produse alimentare care conține 9.835 de tranzacții individuale cu 169 de articole. Primul pas a fost să analizăm elementele din tranzacții și, în special, să trasăm frecvența relativă a celor 25 de articole cele mai frecvente. Acest lucru este echivalent cu suportul acestor articole în care fiecare set de articole conține doar un singur articol. Graficul cu bare ilustrează alimentele care sunt cumpărate frecvent de la acest magazin și este de remarcat faptul că suportul chiar și al celor mai frecvente articole este relativ scăzut (de exemplu, cel mai frecvent articol apare în doar aproximativ 2,5% din tranzacții). Aceste informații au fost folosite pentru a informa pragul minim la rularea algoritmului Apriori; de exemplu, știm că, pentru ca algoritmul să returneze un număr rezonabil de reguli, va trebui să setăm pragul de suport la mult sub 0,025.

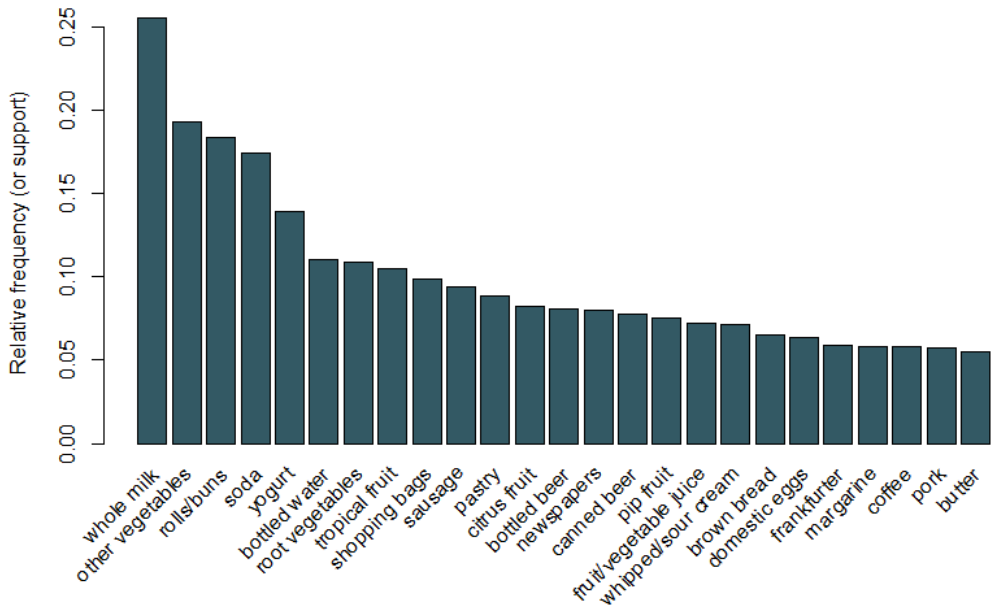

Figura 0.8. Diagrama cu bare pentru valorile celor mai frecvente 25 de articole cumpărate

Setând un prag de suport de 0,001 și încredere de 0,5, putem rula algoritmul Apriori și obținem un set de 5.668 de rezultate. Aceste valori de prag sunt alese astfel încât numărul de reguli returnate să fie mare, dar acest număr s-ar reduce dacă am crește fie pragul, fie suportul. Se recomandă experimentarea cu aceste praguri pentru a obține cele mai potrivite valori. Deși există prea multe reguli pentru a le putea analiza pe toate individual, putem analiza cele cinci reguli cu cea mai mare creștere din tabelul 5.1.

Tabelul 0.1. Cele cinci reguli cu cea mai mare creştere

Rule	Support	Confidence	Lift
{instant food products,soda}=>{hamburger meat}	0.001	0.632	19.00
{soda, popcorn}=>{salty snacks}	0.001	0.632	16.70
{flour, baking powder}=>{sugar}	0.001	0.556	16.41
{ham, processed cheese}=>{white bread}	0.002	0.633	15.05
{whole milk, instant food products}=>{hamburger meat}	0.002	0.500	15.04

Aceste reguli par să aibă sens intuitiv. De exemplu, prima regulă ar putea reprezenta tipul de articole achiziționate pentru un grătar, a doua pentru o seară de film și a treia pentru coacere. În loc să folosiți pragurile pentru a reduce regulile la un set mai mic, este obișnuit ca un set mai mare de reguli să fie returnat, astfel încât să existe o șansă mai mare de a genera reguli relevante. Alternativ, putem folosi tehnici de vizualizare pentru a inspecta setul de reguli returnate și pentru a le identifica pe cele care pot fi utile. Folosind pachetul arulesViz, sunt trasate reguli de încredere, sprijin și ridicare. Acest grafic ilustrează relația dintre diferitele metrici. Regulile optime sunt cele care se află pe ceea ce se numește „granița sprijin-încredere". În esență, ele se află pe marginea din dreapta a diagramei, unde sprijinul, încrederea sau ambele sunt maximizate. Funcția plot din pachetul arulesViz are o funcție interactivă utilă care vă permite să selectați reguli individuale (făcând clic pe punctul de date asociat), ceea ce înseamnă că regulile de la graniță pot fi ușor identificate.

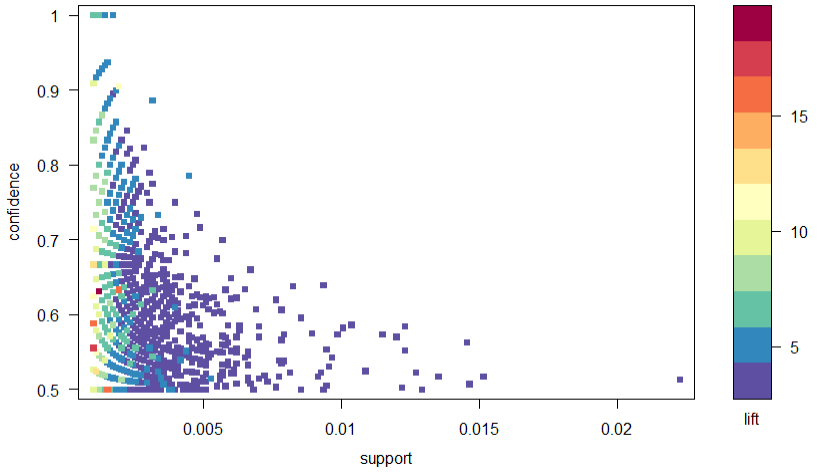

Figura 0.9. Un grafic cu dispersia parametrilor de sprijin, incredere si creştere

Există o mulțime de alte diagrame disponibile pentru a vizualiza regulile, dar o altă figura pe care am recomanda-o să o explorăm este vizualizarea bazată pe grafice a primelor zece reguli în ceea ce privește creșterea (pot fi incluse mai mult de zece reguli, dar aceste tipuri de grafice pot fi cu ușurință

aglomerate). În acest grafic, elementele grupate în jurul unui cerc reprezintă un set de articole, iar săgețile indică relația în reguli. De exemplu, achiziția de zahăr este asociată cu achizițiile de făină și praf de copt. Mărimea cercului reprezintă nivelul de încredere asociat cu regula, iar culoarea, nivelul de ridicare (cu cât este mai mare cercul și cu cât este mai închis gri, cu atât mai bine).

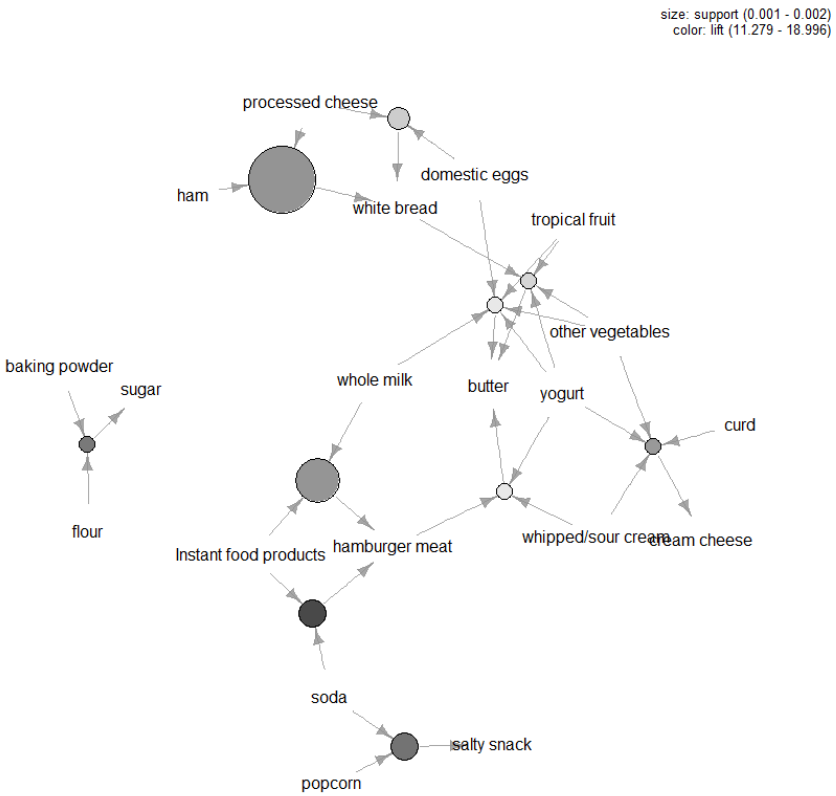

Figura 0.10. Vizualizare bazată pe grafice a primelor zece reguli în ceea ce privește creșterea

Analiza coșului de piață este un instrument util pentru comercianții cu amănuntul care doresc să înțeleagă mai bine relațiile dintre produsele pe care oamenii le cumpără. Există multe instrumente care pot fi aplicate atunci când se efectuează MBA, iar cele mai delicate aspecte ale analizei sunt stabilirea pragurilor de încredere și suport în algoritmul Apriori și identificarea regulilor care merită urmate. De obicei, aceasta din urmă se realizează prin măsurarea regulilor în termeni de metrici care rezumă cât de interesante sunt acestea, folosind tehnici de vizualizare și, de asemenea, statistici multivariate mai formale. În cele din urmă, cheia MBA este să extragi valoare din datele tranzacțiilor tale prin construirea unei înțelegeri a nevoilor consumatorilor tăi. Acest tip de informații este de neprețuit dacă sunteți interesat de activități de marketing precum vânzări încrucișate sau campanii direcționate.

R Code

```
library("arules")
library("arulesViz")
 #Load data set:
data("Groceries")
summary(Groceries)
#Look at data:
inspect(Groceries[1])
LIST(Groceries)[1]
 #Calculate rules using apriori algorithm and specifying support and confidence thresholds:
rules = apriori(Groceries, parameter=list(support=0.001, confidence=0.5))
#Inspect the top 5 rules in terms of lift:
inspect(head(sort(rules, by ="lift"),5))
#Plot a frequency plot:
itemFrequencyPlot(Groceries, topN = 25)
 #Scatter plot of rules:
library("RColorBrewer")
plot(rules,control=list(col=brewer.pal(11,"Spectral")),main="")
#Rules with high lift typically have low support.
#The most interesting rules reside on the support/confidence border which can be clearly seen in this plot.
 #Plot graph-based visualisation:
subrules2 <- head(sort(rules, by="lift"), 10)
plot(subrules2, method="graph",control=list(type="items",main=""))
```

Caz de utilizare : Gestionarea alimentării cu apă folosind cititoare de distanță în rețelele de alimentare cu apă

Protocolul LoRa este o modulare a transmisiei de date fără fir bazată pe tehnologia Chirp Spread Spectrum (CSS) existentă. Prin caracteristicile sale, acesta aparține grupului de protocoale cu consum redus de energie și zonă de acoperire mare (LPWAN). Privind modelul OSI, acesta aparține primului strat fizic. Istoria protocolului LoRa începe cu compania franceză Cycleo , ai cărei fondatori au creat un nou strat fizic de transmisie radio bazat pe modulația CSS existentă. Scopul lor a fost de a oferi schimb de date prin tehnologia fără fir (wireless) pentru contoare de apă, electricitate și gaz. În 2012, Semtech a achiziționat Cycleo și a dezvoltat cipuri pentru client și dispozitivele de acces. Deși până acum modulația CSS fusese aplicată radarelor militare și comunicațiilor prin satelit, LoRa și-a simplificat aplicarea, eliminând necesitatea unei sincronizări precise, odată cu introducerea unui mod foarte simplu de codificare și decodare a semnalelor. În acest fel, prețul chipsurilor a devenit acceptabil pentru utilizare pe scară largă. LoRa folosește spectru de frecvență fără licență pentru lucrarea sa, ceea ce

înseamnă că utilizarea sa nu necesită aprobarea sau închirierea unei concesiuni de la autoritatea de reglementare. Acești doi factori, costul redus și utilizarea gratuită, au făcut ca acest protocol să fie extrem de popular într-o perioadă scurtă de timp.

Modulul EBYTE E32 (868T20D) a fost folosit pentru a crea proiectul. Modulul se bazează pe cipul Semtech SX1276. Puterea maximă de ieșire a modulului este de 100 mW , iar producătorul a declarat o rază de acțiune de până la 3 km folosind o antenă de 5dBi fără obstacole, la o rată de transfer de 2,4 kbps. Acest modul nu are un protocol LoRaWAN integrat , dar este conceput pentru comunicare directă (P2P). Dacă urmează să fie utilizat pentru LoRaWAN , atunci protocolul trebuie implementat pe un microcontroler. Comunicarea dintre modul și microcontroler se realizează prin interfața UART (port serial) și două terminale de control care sunt utilizate pentru a determina starea de funcționare a modulului. Modulul va returna feedback prin instrucțiunea AUX.

LoRaWAN este un protocol software bazat pe protocolul LoRa . Spre deosebire de protocolul de transmisie LoRa legat de brevet , LoRaWAN este un standard industrial deschis operat de organizația nonprofit Alianța LoRa . Protocolul folosește o zonă ISM (Industrie, Știință și Medicină) fără licență pentru activitatea sa. În Europa, LoRaWAN utilizează partea ISM a spectrului care acoperă intervalul între 863 - 870 MHz [4]. Această gamă este împărțită în 15 canale de lățimi diferite. Pentru ca un dispozitiv să fie compatibil LoRaWAN , trebuie să poată utiliza cel puțin primele cinci canale de 125 kHz și să suporte viteze de transmisie de 0,3 până la 5 kbps. Datorită protecției împotriva congestionării frecvenței, ciclul de funcționare al dispozitivului LoRaWAN este foarte scăzut, iar timpul de transmisie nu trebuie să depășească 1% din funcționarea totală a dispozitivului.

Pe lângă definirea tipului de dispozitive și a modului în care acestea comunică prin mesaje, protocolul LoRaWAN definește și aspectul rețelei în sine [5]. Este format din dispozitive finale, de obicei diverse tipuri de senzori în combinație cu dispozitive LoRaWAN . Senzorii apar la transceivere (dispozitive de emisie-recepţie) sau concentratoare centrale. Un senzor poate răspunde la mai multe hub-uri, ceea ce îmbunătățește rezistența și raza de acțiune a rețelei. Hub-urile sunt conectate în rețea la servere care procesează mesajele primite. Una dintre sarcinile serverului este să recunoască mesajele multiple primite și să le elimine. Transceiverele centrale trebuie să poată primi un număr mare de mesaje folosind transceiver radio multicanal și modul adaptiv, adaptându-se la capacitățile dispozitivului final. Securitatea rețelei LoRaWAN este asigurată prin autorizarea senzorului la transceiver-ul central, iar mesajele pot fi criptate între senzor și serverul de aplicații prin criptare AES.

MQTT este un protocol simplu de mesagerie. Este situat în stratul de aplicație al modelului TCP /IP (modele 5-7 OSI). A fost conceput inițial pentru mesagerie în sisteme M2M (mesaj direct între mașini). Principalul său avantaj este nevoia redusă de resurse de rețea și de computer. Din aceste motive, a devenit unul dintre protocoalele principale IoT din lume. Acest protocol se bazează pe principiul

abonamentelor la mesaje și publicării acestora prin intermediari. Un intermediar, numit în mod obișnuit broker, este un server care primește și distribuie mesaje clienților care pot fi editori de mesaje sau pot fi abonați la acestea pentru a le primi. Cei doi clienți nu vor comunica niciodată unul cu altul.

Cel mai important segment al platformei de senzori este fiabilitatea acesteia. Pentru a ne asigura că un accident are loc la timp, trebuie mai întâi să asigurăm fiabilitatea platformei. Tocmai din acest motiv, în soluția propusă în această lucrare se stabilește raportarea periodică de la platforma senzorilor către sistem. Dispozitivul va raporta periodic la fiecare 12 ore, iar de acest lucru se ocupă sistemul de alarmă de pe microcontroler. Și anume, STM32F411 este echipat cu un ceas care monitorizează în timp real (RTC) și oferă posibilitatea de a seta două alarme independente. În acest caz, unul dintre ei se ocupă de trezirea procesului care trimite periodic mesaje cu starea curentă a debitului de apă măsurat prin contor.

Înainte de implementarea software a măsurării, trebuie remarcat faptul că impulsul dat de senzor la tensiunea de ieșire este de 5 V. Deși microcontrolerul utilizat va tolera această tensiune la intrare, este mai bine să o coborâți la valoarea de intrare declarată de 3,3 V. O astfel de tensiune se obține prin două rezistențe, una cu valoarea de 10 kΩ și cealaltă de 22 kΩ , conectate într-un simplu divizor de tensiune [9]. Metoda de conectare este prezentată clar în diagramă. Măsurarea volumului debitului în sine se face prin monitorizarea numărului de impulsuri trimise de senzorul de apă printr-un contor de timp standard. Fiecare impuls va fi înregistrat de microcontroler ca o întrerupere. Când apar impulsuri, este posibil să măsurați debitul și să îl raportați prin transmisie radio LoRa.

Frecvența temporizatorului este setată la 1 MHz printr-un divizor. Comparând numărul de cicluri de ceas dintre cele două întreruperi, se poate obține foarte ușor frecvența pulsului dată de senzorul de debit de apă. Cunoscând frecvența pulsului și caracteristica pulsului, debitul de apă poate fi calculat folosind o procedură predefinită.

Prima valoare măsurată a debitului mai mare decât zero setează platforma senzorului într-o stare de alarmă. Atâta timp cât există un flux, publicitatea periodică va avea loc la fiecare 15 minute în loc de la fiecare 12 ore. La cinci minute după ce fluxul se oprește, dispozitivul va suna la sfârșitul alarmei, iar următorul apel va fi efectuat în mod regulat după 12 ore sau mai devreme în cazul unei noi alarme. Sistemul de alarmă funcţionează intern în aşa fel încât ultima valoare măsurată a debitului de apă să fie citită la fiecare 5 secunde. Această valoare, împreună cu timpul de contor curent, este stocată continuu de procesul de măsurare sub forma unei structuri de timp și debit. Valoarea citită este stocată într-un câmp de dimensiunea a trei elemente. Dacă după trei citiri toate cele trei elemente din câmp sunt egale, se poate determina că în ultimele 15 secunde nu a existat un flux și dispozitivul iese din starea de alarmă. Sistemul așteaptă încă cinci minute înainte de a anunța sfârșitul alarmei prin conexiunea LoRa.

Dacă fluxul se produce din nou în aceste cinci minute, sistemul va acționa ca și cum alarma nu s-ar fi oprit, adică va trimite un mesaj de flux după 15 minute.

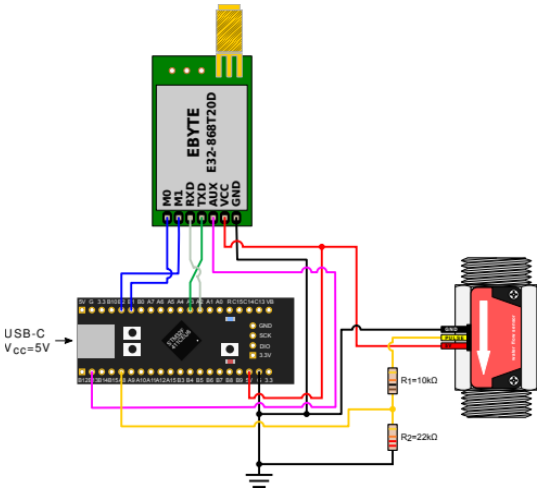

Figura 0.11. Schema de conectare a senzorului pentru debitul de apă

Notificările LoRa sunt întârziate în mod intenționat, astfel încât, în cazul apariției constante și întreruperii fluxului, acestea nu ar trimite adesea mesaje radio.

Experiența de viață reală

În timpul măsurării, circuitul este alimentat cu 5 V DC. Aceasta este tensiunea de funcționare recomandată pentru modulul LoRa și senzorul de debit de apă utilizat, în timp ce microcontrolerul poate fi alimentat cu 5 V sau 3,3 V. În această măsurătoare, primul obiectiv este să arate că valoarea curentului de vârf nu va atinge o valoare mai mare. de 300 mA, care este maximul pe care îl poate suporta circuitul microcontrolerului. Aceste date ne permit să alimentam întregul circuit prin microcontroler folosind portul USB încorporat și astfel simplificăm aspectul întregului senzor. Al doilea obiectiv este reducerea consumului de energie pentru a prelungi cât mai mult autonomia de funcționare a senzorului. Ca sursă de alimentare externă, a fost folosită o sursă de alimentare de laborator R-SPS3010 de la Nice-power, care poate asigura o tensiune de funcționare stabilă de la 0 la 30 V cu un curent de până la 10 A. Instrumentul de măsurare universal UT139B de la UNI-T este conectat în serie. Este setat să măsoare miliamperi în timpul măsurării, păstrând valoarea maximă măsurată pe ecran.

Măsurarea domeniului

Intervalul a fost măsurat de la așezarea Zagreb Vrbani 3, care este situată lângă Lacul Jarun. Această locație ne oferă o perspectivă asupra intervalului de așteptare în mediul urban și în mediul rural. Și anume, de la transceiver-ul central spre nord există o parte foarte urbană, cu multe clădiri rezidențiale și infrastructură de trafic dens, în timp ce pe partea de sud se află Lacul Jarun și râul Sava, care sunt în mare parte zone verzi, păduri mai mici și doar câteva clădiri mai mici de înălțime. Factorul limitativ este

poziția antenei transceiver-ului central, care era amplasată la primul etaj al unei clădiri de locuințe, la aproximativ 4 m deasupra nivelului solului și înconjurată de clădiri. La măsurarea pe partea laterală a transceiver-ului central, a fost folosită o antenă omnidirecțională cu un câștig de 3,5 dB, care este staționară, amplasată în exteriorul ferestrei unei clădiri rezidențiale. Pe partea senzorilor, pentru mobilitate, a fost folosită o antenă mai mică, cu câștig de 2 dB. Semnalul a fost trimis în mod deschis „din sub control". Poziția fiecărei măsurători a fost înregistrată printr-un dispozitiv GPS pe un dispozitiv mobil și ulterior transferată pe Google Earth. În Google Earth, este posibil să importați puncte de măsurare înregistrate și să măsurați distanța dintre acestea și antena transceiver-ului central. Conform specificaţiilor producătorului, raza maximă de acţiune care se poate aştepta de la aceste module este de 3 km în condiţii aproape ideale cu o antenă de 5 dB. Pentru a aborda cumva această distanță în ciuda poziției nefavorabile de măsurare, rata de transfer de date a fost redusă de la setările standard ale modulului de la 2,4 kbps la 300 bps. Datorită cantității mici de date care trebuie transmise, acesta nu este un factor limitativ în practică, iar datorită vitezei reduse de transmisie, s-a obținut o cantitate mai mică de erori la recunoașterea semnalului primit și un succes crescut în primirea mesajelor pe distanţe lungi. În figura de mai jos este prezentat intervalul măsurat al sistemului LoRa fabricat. Poziția transceiver-ului central este afișată cu un asterisc, în timp ce punctele din care semnalul de la senzor a reușit să-l ajungă sunt colorate cu verde. Punctele roșii indică locurile în care nu a fost posibilă comunicarea între senzor și transceiver-ul central. După cum era de așteptat, cea mai mare rază de acțiune de 3393 m a fost atinsă spre sud-est, unde în afară de câteva clădiri rezidențiale din apropierea antenei, nu au existat obstacole suplimentare. Spre sud-vest, rezultatul obtinut a fost de 2773 m. Cu toate acestea, conform zonei urbane a orașului, raza maximă de acțiune realizată a fost de 982 m la est, iar la nord a fost de doar 860 m.

Figura 0.12. Poziția antenei centrale de emisie-recepţie central și domeniul de măsurare

Conform specificației, consumul maxim al modulului utilizat este de 130 mA. Consumul măsurat al senzorului de debit de apă este de 4 mA. Curentul maxim care poate fi admis prin placa de dezvoltare a plăcii senzorului este de 300 mA, iar circuitul de pe platforma de dezvoltare utilizată este proiectat astfel încât terminalul USB Vbus și bornele de 5 V ale circuitului să fie pe aceeași magistrală. Din aceasta putem concluziona că întreaga interfață cu senzorul și modulul LoRa poate fi alimentată de interfața USB. Cu toate acestea, este necesar să se optimizeze consumul, astfel încât circuitul să poată funcționa pe o baterie disponibilă în comerț cât mai mult timp posibil. Tabelul 5.2 prezintă măsurătorile curente

în timpul funcționării microcontrolerului. Aici, microcontrolerul a funcționat cu un ceas de funcționare maxim de 96 MHz și fără nicio optimizare a puterii. Datele sunt date separat pentru fiecare element pentru a facilita urmărirea optimizării.

Tabelul 0.2. Curentul din circuite fără optimizare

Connected system components	Current [mA]	State
Microcontroller	26.65	Wait
Microcontroller	26.88	Event stop
Microcontroller + LoRa Module	39.16	Wait
Microcontroller + LoRa Module	121.5	Signal send
Microcontroller + LoRa Module + Sensor	42.51	Wait
Microcontroller + LoRa Module + Sensor	125.7	Signal send

Întrucât senzorul de debit nu are posibilitatea de optimizare, în Tabelul 5.2 sunt evidențiate valorile curentului care circulă prin acesta și la sfârșitul fiecărei etape se vor adăuga doar la rezultatele obținute. Tabelul 5.2 arată că prin reducerea ceasului de funcționare, curentul a scăzut cu 11 mA, ceea ce reprezintă o scădere cu puțin peste 40% a consumului microprocesorului.

Table 0.3. Curentul prin senzorul de apă

Current [mA]	State
3.35	Idle
4.03	Flow

Primul pas al optimizării este să scazi tactul de ceas al procesorului la 48 MHz.

Table 0.4. Curentul cu frecvența tactului de ceas al microprocesorului redusă

Connected system components	Current [mA]	Stanje
Microcontroller	15.50	Wait
Microcontroller	15.91	Event stop
Microcontroller + LoRa Module	28.15	Wait

Deoarece modulul LoRa de pe platforma senzorului nu este utilizat pentru primirea mesajelor, nu este nevoie să-l mențineți activ în mod constant. Din fericire, acest modul are un mod în care își închide transceiver-ul radio. Prin schimbarea codului de pe microcontroler a fost introdus un mod de operare în care transceiver-ul radio este pornit doar atunci când este necesar. Cu această procedură, curentul total prin microcontroler și modulul LoRa a scăzut la 17,7 mA în modul de așteptare. Microcontrolerul STM32F411 are diverse funcții de economisire a energiei. Una dintre ele este o stare de somn în care oprim complet ceasul procesorului și ascultăm doar întreruperile provenite de la dispozitive sau ceasuri

externe. Deoarece FreeRTOS a fost folosit în lucrare, în loc să trimită direct microprocesorul în stare de repaus, FreeRTOS a fost folosit în modul fără tact de ceas. În el, FreeRTOS nu mai funcționează și pune microprocesorul în stare de adormire. Acest lucru scade curentul prin circuitul format din microcontroler și modulul LoRa la 5,87 mA în modul de așteptare, curentul total prin întregul circuit fiind acum de doar 9,22 mA în modul de așteptare. Măsurarea intensității curentului a arătat cu succes cum este posibil să folosiți un port USB pentru a alimenta întregul circuit. De asemenea, în mai multe intervenții asupra codului de program al microprocesorului a fost posibilă scăderea curentului de la 42,51 mA la 9,22 mA, ceea ce reprezintă o diferență de 78%. Acest lucru este foarte important deoarece timpul de așteptare este starea în care se află circuitul aproape tot timpul. Folosind un încărcător USB portabil (power bank) cu o capacitate de 10000 mAh (cea mai comună valoare la momentul scrierii), cu un astfel de consum se poate conta pe aproximativ 40 de zile de funcționare autonomă a senzorului. Achiziţia semnalului radio a dat rezultate foarte bune având în vedere puterea şi poziţia antenei. Această măsurătoare este un indiciu al faptului că, chiar și fără o căutare mare a poziției ideale a antenei, se poate obține o gamă destul de decentă cu un dispozitiv care are puterea de ieșire a unui sistem Wi-Fi de acasă obișnuit. Distanța maximă măsurată a fost de 3393 m în ceea ce privește măsurătorile de la nivelul solului și fără vizibilitate optică. Există, de asemenea, o mare diferență în comportamentul protocoalelor radio LoRa între zonele urbane și cele rurale. În timp ce într-o zonă nelocuită gama a depășit specificațiile producătorului, în locurile cu mai multe clădiri rezidențiale, gama a scăzut brusc. Se poate concluziona că, în scopul raportării evenimentelor adverse din zonele rurale și îndepărtate, LoRa LPWAN este o soluție excelentă. Raza mai mică în zona urbană este foarte ușor de compensat cu transceiver-uri centrale mai dense.

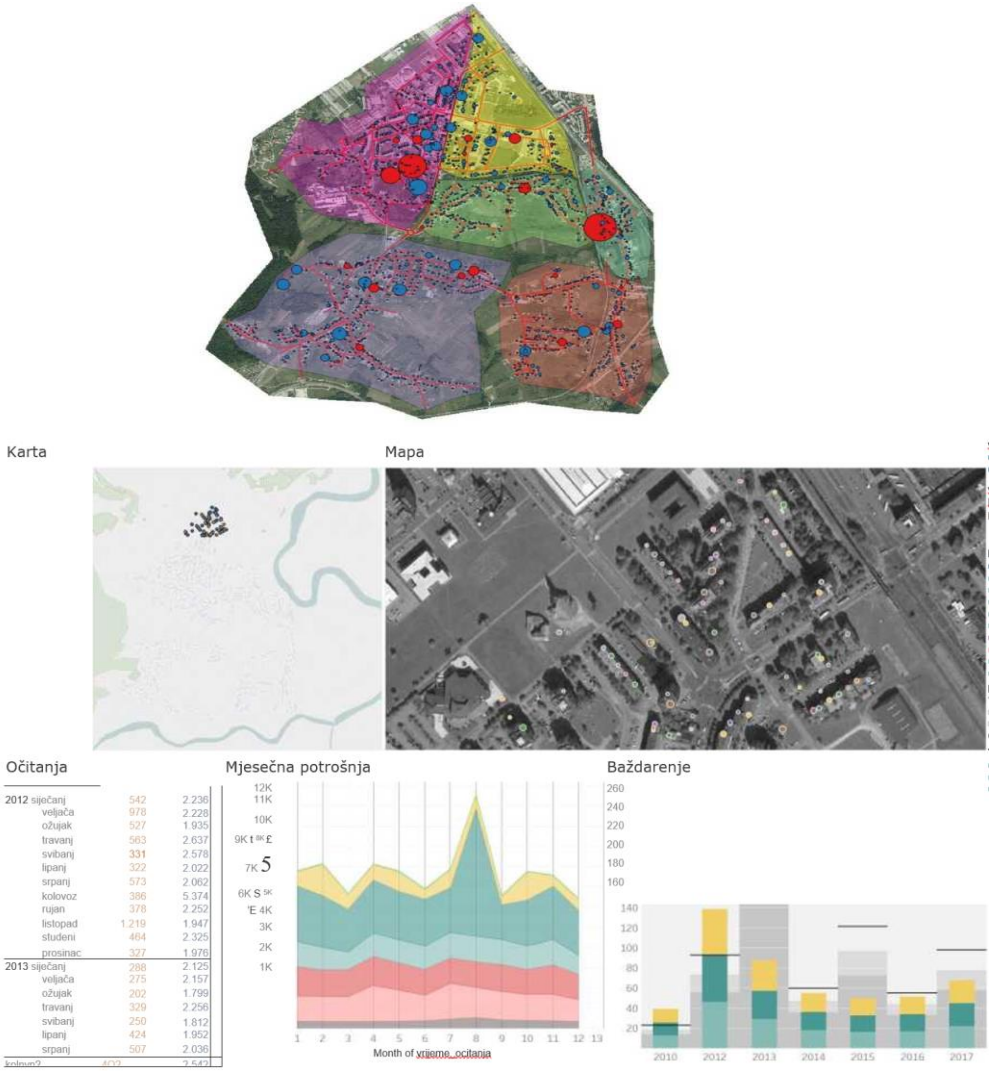

Figura 0.13. LoRa LPWAN

Caz de utilizare: clasificarea site-urilor de phishing pe bază de reguli

Înainte de instruirea modelului de clasificare a fost necesar să se aleagă caracteristicile care sunt relevante și utile pentru procesul de clasificare. Pentru a evalua caracteristicile, am folosit clasarea caracteristicilor pe baza următoarelor metode:

- Câștig de informații care clasifică caracteristicile pe baza câștigului de informații calculat în raport cu clasa de clasificare, caracteristicile numerice sunt mai întâi discretizate.
- Raportul de câștig clasifică caracteristicile pe baza raportului de câștig calculat. Raportul de câștig este calculat ca câștig de informații împărțit la entropia caracteristicii pentru care este calculat raportul.

- Incertitudinea simetrică este o măsură care elimină caracteristicile redundante și lipsite de sens, care nu au interconectivitate cu alte caracteristici.
- Metoda de relief a fost propusă de Kira și Rendell și este folosită pentru selectarea caracteristicilor relevante statistic, este rezistentă la zgomot în dana și interdependența caracteristicilor.

Caracteristicile sunt evaluate într-un mod care este eșantionat aleatoriu dintr-un set dat de instanțe și iau cei mai apropiați vecini care aparțin clasei. Dacă vecinii sunt aliniați cu instanțe, factorul de ponderare crește, în contrast, dacă cei mai apropiați vecini sunt diferiți, factorul de ponderare scade.

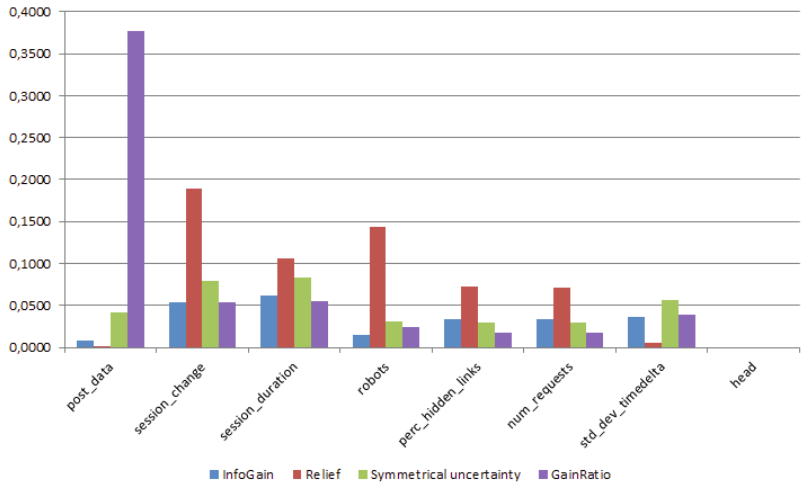

Figura 0.14. Compararea diferitelor metode de selectare a caracteristicilor

Dacă ne uităm la caracteristicile clasificate, vedem următoarele caracteristici care domină setul de date:

- date postate, care ne arată dacă clientul a completat/nu a completat forma falsă
- în sistemul Lino
- schimbarea sesiunii, care ne arată dacă utilizatorul, în timpul sesiunii, a schimbat identificatorul de sesiune sau nu
- durata sesiunii, durata sesiunii în secunde
- roboţi, care ne arată dacă utilizatorul a accesat/nu a accesat fişierul robots.txt,
- care definește regulile de conduită a robotului.

Caracteristicile menționate mai sus au fost selectate manual, am clasificat toate caracteristicile în funcție de scorul metodei de selecție a caracteristicilor. Am selectat cele mai semnificative caracteristici pentru modelele noastre de clasificare, în cazul nostru primele cinci caracteristici.

Selecția modelului de clasificare pentru bot din diferențierea umană

O condiție prealabilă pentru utilizarea metodelor de învățare supravegheată și selectarea subsetului optim de caracteristici este un set de date etichetat. Caracteristicile selectate ar trebui să contribuie la generalizarea unor clase, adică pentru fiecare clasă ar trebui să se poată realiza un profil comportamental unic. Pentru a evalua performanța metodei de clasificare am folosit metoda de validare încrucișată K-fold. Pentru scopurile noastre am folosit k = 10 părți - literatura relevantă afirmă că k = 10 părți sunt un număr optim pentru estimarea erorilor.

Arborele de decizie C 4.5

În primul rând, în scopuri de clasificare, am evaluat un algoritm de arbore de decizie C 4.5, care este o actualizare a algoritmului clasic ID3. Ambii algoritmi sunt rezultatul cercetărilor efectuate de Ross Quinlan. C 4.5 folosește un set de date pentru a învăța să creeze un arbore redundant. În cazul utilizării datelor similare, în procesul de învățare și validare.

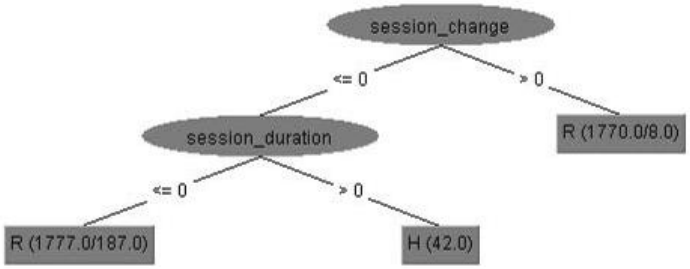

Figura 0.15. Arborele tăiat, folosind setul complet de caracteristici

Clasificatorul are rezultate bune, dar atunci când folosim un set de validare independent, clasificatorul produce de obicei rezultate proaste.

După construirea unui arbore redundant, arborele este convertit la regulile IF/THEN și algoritmul calculează cele mai bune condiții pentru acuratețea clasificării, eliminăm condițiile IF dacă acestea nu reduc precizia clasificării. Tăierea se face de la frunze până la rădăcina arborelui și se bazează pe estimarea pesimistă a erorilor; erorile sunt legate de procentul de cazuri clasificate incorect din setul de date de instruire. Pe baza diferenței de precizie a regulilor și a abaterii standard luate din distribuția binomială definim o anumită limită superioară de încredere care este de obicei 0,25, pe baza căreia arborii sunt tăiați. Pentru a construi modelele noastre cu C 4,5, am stabilit pragul de încredere pentru tăiere la 0,25 și numărul minim de instanțe pe frunză este 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

Figura 0.16. Rezultatele clasificării pentru C 4.5 și SVM, experimentul 1 utilizează numai caracteristicile selectate. Experimentul 2 folosește caracteristicile selectate plus Țara și ASN-ul clientului

Înainte de clasificare, am eliminat instanța de clasă a vizitatorilor necunoscuți, deoarece aceștia reprezentau încercări umane de a ataca cu vale introduse manual sau folosind browsere inexistente. Metoda C 4.5 a dus la afișarea arborelui tăiat, care este același cu selecția optimă a caracteristicilor și utilizarea setului complet de caracteristici. Este important de remarcat faptul că algoritmul C 4.5 este foarte bun la alegerea caracteristicilor prin utilizarea euristicii în crearea și ștergerea subarborilor.

Dacă ne uităm la rezultatele din Tabel, putem vedea că pentru caracteristicile date (Experimentul 1) avem o precizie de clasificare de 94,5% și o rată perfectă de pozitive corecte pentru roboți (rata TP). Clasificatorul clasifică prost vizitatorii umani (TPR = 0,177) și degradează capacitatea de clasificare a robotului în cazul în care rata este fals pozitiv rata este mare - 0,823. Privind la măsura F, putem spune că un bun clasificator detectează corect roboții, în timp ce clasifică greșit vizitatorii umani și de obicei (> 80%) îi declară roboți. Am testat C 4.5 mai elegant si mai sofisticat cu două caracteristici suplimentare - țara clientului și ASN-ul furnizorului de servicii. Aceste caracteristici au fost rezolvate de la adresa IP folosind baza de date GeoIP menționată mai sus. Acest subset (C 4.5 Experimentul 2) este prezentat în tabel. Am redus numărul de fals pozitive pentru clasa Robot la 0,207, astfel rezultatul clasificării pentru clasa Uman a fost mai bun 0,793.

Suport Vector Machine

SVM este un algoritm care găsește marja maximă de separare între clase, definind în același timp marja ca distanța dintre punctele critice care sunt cele mai apropiate de suprafața de separare. Punctele cele mai apropiate de suprafață sunt numite vectori de sprijin, marginea M poate fi văzută ca lățimea separării dintre suprafețe. Calcularea vectorului suport este o problemă de optimizare care poate fi rezolvată folosind diferiți algoritmi de optimizare. Trucul folosit în calcularea SVM este utilizarea diferitelor funcții ale kernel-ului, care mută problemele nerezolvabile sau inadecvate într-o dimensiune mai înaltă, unde pot fi rezolvate. În experimentele noastre, am antrenat modelele noastre SVM cu

algoritmul secvenţial de optimizare minimă folosind un nucleu liniar *K* (*x, y*) = < *x* ,*y* > unde _ = 1 . 0 - 12 iar toleranța este setată la 0,001, datele anterioare de antrenament au fost normalizate. Pentru, caracteristicile experimentului 1, SVM performează mai bine decât C 4.5, precizia a fost de 95,8 %. Vizitatorii umani sunt încă o problemă, deși SVM are o rată mult mai mare de pozitive adevărate (26,5 %). Rata crescută de detecție a vizitatorului uman oferă o rată mai mică de detectare greșită a roboților (73,5 %). Măsura F este foarte bună pentru roboți și mult mai bună pentru vizitatorii umani (chiar mai bună decât metoda C 4.5) - dar încă prea mică pentru a fi folosită - (0,419). Cu funcții suplimentare Țară și ASN (Expertiment 2) am obținut o rată falsă pentru ambele clase sub 5%. Rata adevărată pozitivă a fost, de asemenea, mare pentru clasa Uman 0,962 și pentru clasa Robot 0,998. Putem concluziona că, cu acest subset de caracteristici și cu reinstruire regulată pentru a evita deriva conceptului, acest model este fezabil pentru utilizarea zilnică.

Caz de utilizare : sistem bazat pe cloud pentru prevenirea pierderii datelor

Comparația soluțiilor DLP disponibile pe piață

Comparație a soluțiilor DLP disponibile pe piață, bazată pe Gartner Gartner ® Releases 2022 Market Guide for Data Loss Prevention: Key Takeaways.

Symantec

Întemeiat în Mountain View, California, Symantec se află pe piața DLP de la achiziția Vontu în 2007. Symantec a lansat recent Symantec Data Loss Prevention 15.0 și are produse componente pentru DLP Enforce, DLP IT Analytics, stocare în cloud (suportă mai mult de 65 de aplicații cloud), Cloud Prevent pentru Microsoft Office 365, DLP pentru punct final, DLP pentru stocare în rețea și DLP, precum și suport pentru tehnologie de securitate terță parte DLP API, cum ar fi regăsirea conținutului, raportarea și FlexResponse pentru criptarea conținutului sau aplicația DRM. Symantec continuă să investească în tehnologia DLP și își îmbunătățește unitatea de afaceri pentru protecția datelor. În 2016, Symantec a achiziționat Blue Coat, ceea ce îi oferă opțiunea de a achiziționa Elastica și Perspecsy pentru Blue Coat, pentru care există integrarea politicilor DLP prin API-ul REST bidirecțional între Elastica și Symantec DLP. Symantec este o alegere convenabilă pentru organizațiile care necesită tehnici avansate de detectare și integrare cu CASB pentru o politică unică de protecție a datelor.

Avantaje

Symantec oferă cele mai avansate tehnici de detectare de pe piață, cu funcționalități avansate, cum ar fi recunoașterea formularelor, analiza imaginilor și recunoașterea scrisului de mână, care pot acoperi o gamă largă de scenarii de pierdere de date. Symantec acceptă un model de implementare hibrid pentru mai multe dintre produsele sale DLP în care serverele de detectare instalate pe AWS, Azure sau Rackspace se conectează la o platformă locală DLP Enforce. Sistemul SmartResponse de la Symantec oferă o gamă largă de flexibilitate administrativă bazată pe acțiuni de conținut care sunt conforme cu regula DLP. DLP-ul său Vector Machine Learning (VML) le permite utilizatorilor să învețe sistemul DLP, oferind atât conținut pozitiv, cât și negativ. Acest lucru ar putea fi util dacă metodele tradiționale de potrivire nu sunt suficiente pentru a potrivi corect conținutul.

Puncte slabe

Clienții Symantec și-au exprimat frustrarea când au cumpărat sau actualizat pluginuri Data Insight pentru Symantec DLP, care este acum deținut de Veritas. Asigurați-vă că furnizorul dvs. Symantec DLP poate vinde și Veritas Data Insight dacă sunteți interesat de acest supliment. Monitorizarea și detectarea datelor sensibile în aplicațiile cloud necesită detectarea punctului final DLP și conectorii Symantec CASB necesari pentru a obține funcționalitatea completă. Clienții își exprimă îngrijorarea față de costul total al implementării Symantec DLP, în comparație cu produsele concurente.

Guardian digital

Înființată în 2002, Digital Guardian (fostă Verdasys) are sediul în Waltham, Massachusetts. Accesul la Digital Guardian DLP se face în principal prin intermediul terminalului DLP, cu parteneriate puternice pentru integrarea rețelei de produse DLP și detectarea DLP până în octombrie 2015, când Code Green Networks (CGN) a fost dobândită prin achiziție. De atunci, a lansat-o ca o linie de produse Digital Guardian Network DLP. Punctul final Digital Guardian acoperă DLP, protecție avansată împotriva amenințărilor și detectarea și răspunsul punctelor finale (EDR) într-un singur agent instalat pe computere desktop, laptopuri și servere care rulează pe Windows, Linux și Mac OS X, precum și suport pentru mediile VDI. Digital Guardian Network DLP și produsul Digital Guardian Discovery acoperă rețelele DLP, protecția datelor în cloud și descoperirea datelor și sunt oferite ca hardware, aplicații software și/sau aplicații virtuale. Pe parcursul anului 2016, Digital Guardian a lucrat la simplificarea și integrarea capabilităților de management între punctele sale finale DLP și activele din achizițiile CGN. Digital Guardian are, de asemenea, un parteneriat existent cu Fidelis Cybersecurity Network DLP. Mai mulți clienți Gartner au vorbit recent despre acest parteneriat, iar Gartner consideră că, pe lângă clienții comuni existenți, parteneriatul va continua să se reducă și în cele din urmă va înceta. Digital Guardian este o alegere potrivită pentru organizațiile cu preocupări puternice cu privire la legislație, în special în sectorul sănătății și serviciile financiare, precum și pentru organizațiile cu cerințe de protecție AD a proprietății intelectuale. Digital Guardian este, de asemenea, o alegere bună pentru organizațiile care necesită uniformitatea regulilor DLP pentru a funcționa la fel de bine în toate sistemele de operare Windows, Mac OS X și Linux.

Avantaje

Clienții raportează timpi de implementare mai rapizi și proiecte de succes atunci când folosesc produsul Digital Guardian în combinație cu serviciile gestionate de Digital Guardian. Digital Guardian are integrare cu produse de securitate mai largi, inclusiv informații despre amenințări, sandbox de rețea, Analiza utilizatorilor și entităților (UEBA), Protecția datelor în cloud și Managementul evenimentelor de securitate (SIEM, inclusiv aplicațiile IBM QRadar și Splunk) . Clienților le place opțiunea de licențiere modulară pentru punctul final DLP, cu suport pentru Windows, Mac OS X și Linux, și punctele finale care pot fi licențiate în orice combinație de vizibilitate și control al dispozitivului, DLP și protecție avansată

împotriva amenințărilor. Viziunea Digital Guardian arată o înțelegere puternică a tehnologiei, securității, amenințărilor și tendințelor din industrie care le vor modela licitarile.

Puncte slabe

Digital Guardian nu are o politică comună pentru punctele finale și produsele de rețea. Agentul Digital Guardian nu poate face diferența între conturile personale și cele de afaceri pentru Microsoft OneDrive. Cu toate acestea, poate preveni utilizarea aplicațiilor personale Microsoft OneDrive. Clienții și-au exprimat preocuparea cu privire la viteza de integrare a CGN-ului achiziționat. Indexarea datelor structurate nu este sprijinită de agentul punct final Digital Guardian, dar această caracteristică este disponibilă prin agentul CGN.

Punct de forță

În 2015, Raytheon și Vista Equity Partners au încheiat o societate mixtă care combină Websense, o companie din portofoliu Vista Equity și Raytheon Cyber Products. În 2016, compania a câștigat două linii de Intel Security - Stonesoft și Sidewinder fireworks prin achiziție - și a repornit compania combinată ca Forcepoint. Raytheon deține deja acțiunile municipale Forcepoint, iar Vista Equity Partners deține un pachet minoritar. Cu sediul central în Austin, Texas, Forcepoint este lider pe piața de produse DLP, cunoscută anterior ca Raytheon-Websense, de câțiva ani. Linia de produse Forcepoint DLP include Forcepoint DLP Discover, Forcepoint DLP Gateway, Forcepoint Cloud Applications și Forcepoint DLP Endpoint. Pe parcursul anilor de livrare a DLP și a modulelor DLP integrate pentru produsele sale securizate de gateway web și e-mail, Forcepoint a creat un pachet DLP remarcabil pentru acoperirea rețelei, punctele finale și descoperirea datelor (atât client, cât și cloud), cu o atenție deosebită protecției de proprietate intelectuală și implementarea politicii de conformitate cu reglementările. Forcepoint este o alegere potrivită pentru organizațiile cu cerințe de conformitate cu legislația și protecția proprietății intelectuale sau organizațiile care doresc să implementeze dispozitive virtuale DLP în infrastructura Azure public cloud.

Avantaje

Forcepoint DLP Endpoint poate cripta/decripta automat fișierele prin Microsoft RMS fără a elimina protecția RMS pe baza datelor end-to-end, a datelor de mișcare și a regulilor de descoperire. Forcepoint oferă peste 350 de reguli predefinite și componenta încorporată UEBA pentru caracteristici analitice de securitate suplimentare care realizează evaluarea riscului de incident, identifică amenințările de la utilizatorii interni, evidențiază punctele finale pe cale de disparitie și calculează indicatorii de risc de furt de date pentru a identifica cei mai vulnerabili utilizatori și activități. Indexarea datelor structurate, în special suportul pentru indexarea datelor în Salesforce, citează clienții ca factor cheie de diferențiere.

Puncte slabe

Clienții au raportat probleme cu suportul tehnic pentru indexarea datelor structurate. Dacă trebuie să indexați date structurate în baza de date, asigurați-vă că le testați temeinic pe date reale din mediul dumneavoastră specific de bază de date. Implicarea Raytheon pe piața de apărare va ajuta la consolidarea Forcepoint cu informații și produse suplimentare. Cu toate acestea, nu există succes al vânzătorilor de securitate deținuți de structurile de apărare care au reușit pe piețele comerciale. Relevanța lui Forcepoint în unele zone geografice poate fi problematică din cauza loialității puternice americane a lui Raytheon. Unii clienți Gartner au notat această reclamație și văd dacă aceasta provoacă îngrijorări în organizația dvs.

Intel Security (azi: McAfee)

De-a lungul ultimilor ani, Intel și-a schimbat de mai multe ori investițiile în și din diverse linii de produse și nu a luat în considerare suficient aceste schimbări în interiorul și în afara companiei. Acest lucru a provocat epuizarea angajaților la ritmuri alarmante, dintre care mulți au fost lansaţi de noi companii de securitate sau sunt angajați de furnizori de securitate competitivi. Din punct de vedere istoric, în multe dintre produsele de securitate Intel, a existat o lipsă cronică de investiții.

Abordarea de securitate a Intel a fost să integreze achizițiile cu sistemul de management al politicilor McAfee ePolicy Orchestrator (McAfee ePO), monitorizarea alertelor și conectarea evenimentelor de securitate între sfârșiturile de evenimente DLP, transferurile de rețea și datele restricționate privind datele de stocare din organizație. Versiunea DLP 10.0 a adus noi îmbunătățiri DLP, iar actualizările produselor DLP online din 2016 au evidențiat accentul reînnoit al McAfee pe protecția datelor. Intel Security este o alegere bună pentru organizațiile care au resurse semnificative investite în McAfee ePO și doresc un furnizor unic care poate oferi DLP, controlul dispozitivelor și criptarea.

Avantaje

Integrarea DLP în proxy McAfee Web Gateway acceptă decriptarea și re-criptarea traficului site-ului, inclusiv furnizorii de servicii de e-mail și produsele de stocare în cloud. Baza de date de captură poate indexa și stoca toate componentele vizibile ale rețelei și punctelor finale. Clienții au raportat acest lucru util pentru a testa reguli noi, analiza criminalistică a evenimentelor care au avut loc înainte de elaborarea politicilor și investigarea după eveniment. De asemenea, acceptă descoperirea electronică și reţinerea moștenirii, precum și integrarea directă cu software-ul Guidance Software și AccessData. McAfee DLP include nivelul de bază al clasificării datelor pe punctul final DLP 10 pentru Windows și Mac OS X și poate fi în continuare integrat cu fermitate cu Titus și Bold James pentru diferite opțiuni de clasificare a datelor. Regulile punctelor finale DLP sunt conștiente de locații și pot avea răspunsuri și remedii de conținut diferite atunci când sunt online sau sunt offline. Federația Inovațiilor în Securitate (SIA) este încă robustă și este o modalitate bună pentru clienții Intel Security de a-și maximiza investiția

în DLP datorită integrării dovedite și testate a clasificărilor produselor de date, a furnizorilor DRIF și UEBA.

Puncte slabe

McAfee DLP sprijină nativ integrarea API cu Cloud Data Box, dar suportul pentru alte aplicații cloud și suportul pentru stocarea în cloud lipsesc. Intel Security a facut unele îmbunătățiri la DLP Agent 10 pe Mac OS X, dar încă lipseste sprijinul pentru e-mail, web și cloud. Linux nu este acceptat. Clienții raportează că configurarea regulilor DLP poate fi complexă și dezavantajoasă în comparație cu alte produse DLP. Succesul viitor al Intel Security pe piața DLP va depinde de performanța acestora în timp ce acționează ca companie și de faptul că accentul se poate pune pe sarcinile de securitate a datelor pe o perioadă mai lungă de timp.

Caz de utilizare: Găzduire dinamică a site-urilor web

Inspirat de: https://www.linkedin.com/pulse/host-dynamic-website-aws-sara-mostafa/

Cum să implementați un site web dinamic cu AWS prin încărcarea conținutului site-ului dvs. în bucket-ul S3, creați o instanță EC2 pentru a găzdui aplicația web pe aceasta, deoarece în acest scenariu EC2 acționează ca un server public, toți oamenii din lume pot vizita acest server.

Amazon S3 (Simple Storage Service –serviciu de depozitare simplă) este un serviciu oferit de AWS pentru stocarea obiectelor printr-o interfață de serviciu web. Poate fi folosit pentru a stoca sau a recupera orice cantitate de date, cum ar fi documente, imagini, videoclipuri etc.. S3 bucket este o resursă în Amazon S3. Este un container în care pot fi încărcate fișiere și foldere.

Amazon EC2 (Elastic Compute Cloud) este un serviciu oferit de AWS. Este considerat un server virtual. IAM (Identity and access management) Rolul este folosit pentru a acorda permisiunea serviciului de a face ceva într-un alt serviciu.

Serverul web LAMP poate fi folosit pentru a găzdui un site web static sau pentru a implementa o aplicație PHP dinamică care citește și scrie informații într-o bază de date.

Pași

Pasul 1: Creați bucket-ul S3

Va trebui să creați un bucket S3 pentru a pune fișierele și folderele site-ului dvs. web. Pentru a face acest lucru, autentificați-vă la consola de management AWS și faceți clic pe Servicii din bara de navigare de sus . Din meniul drop-down Servicii, selectați S3 din secțiunea Stocare. Aceasta ar trebui să afișeze dashboard (tabloul de bord) S3.

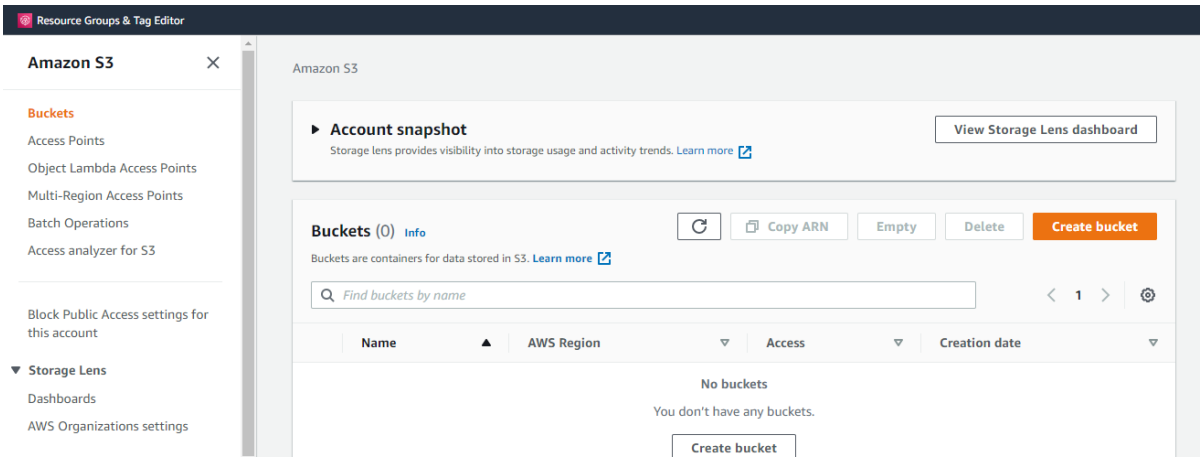

Figura 0.17. Crearea unui bucket S3 – primul pas

Din dashboard (tabloul de bord) S3, faceți clic pe Create bucket (Creare bucket). Dați bucket-ului un nume unic, numele pe care îl alegeți trebuie să fie unic la nivel global. Apoi, alegeți regiunea AWS preferată din meniul drop-down.

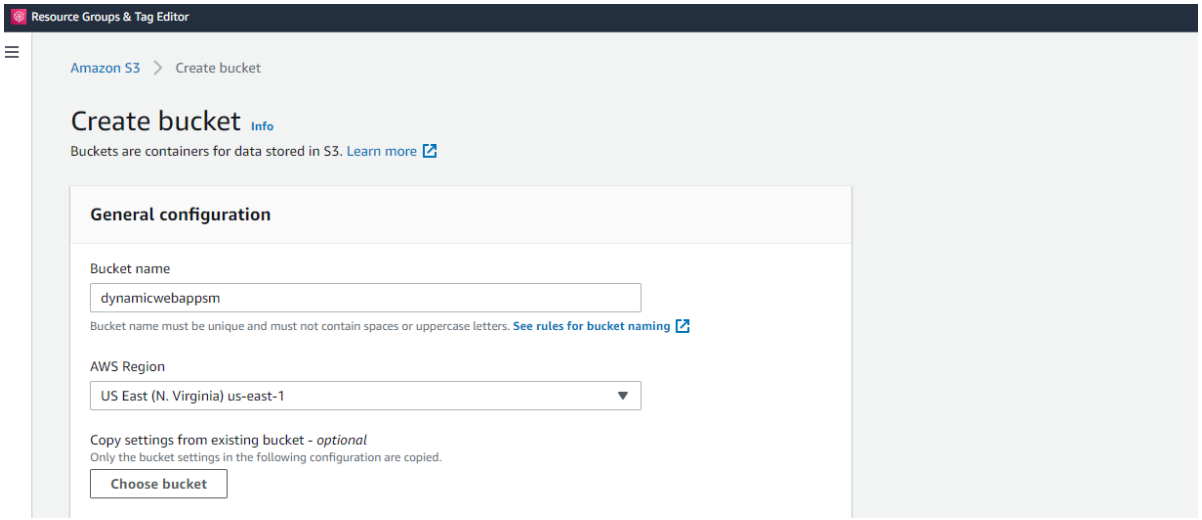

Figura 0.18. Crearea unui bucket S3 – pasul doi

Sub "Block Public Access settings for this bucket" (setările blocare a accesului public pentru aceast bucket), bifați caseta de selectare "Block all public access" (Blocare totală pentru accesul public). Acest lucru se face pentru ca bucket-ul să nu fie accesibil publicului.

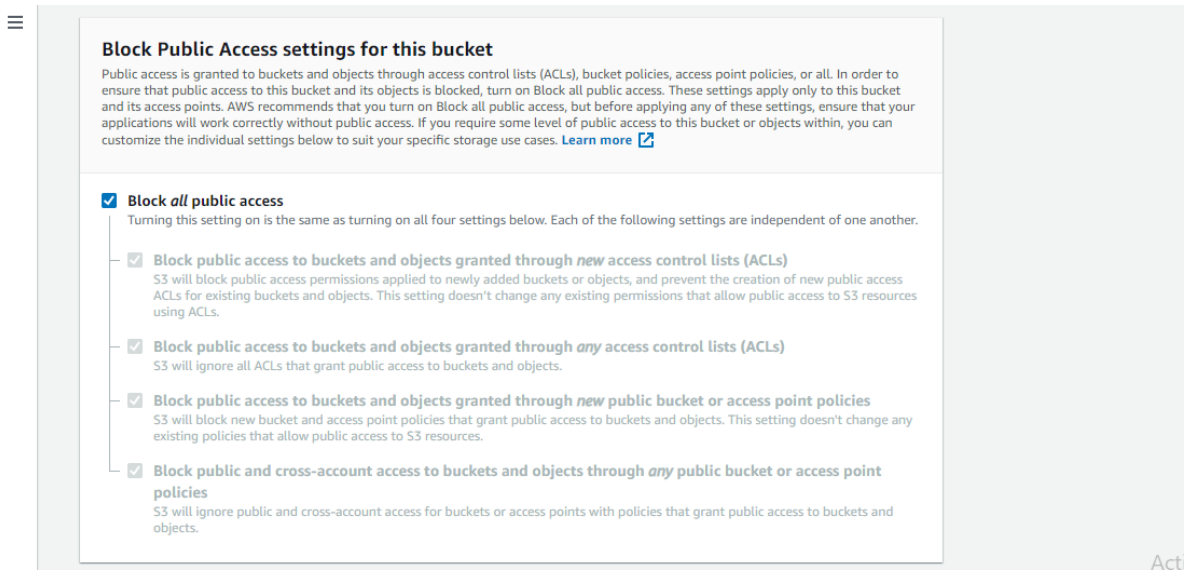

Figura 0.19. Crearea unui bucket S3 – pasul trei

Faceți clic pe "Disable (Dezactivare)" din caseta "Bucket Versioning (versiunea bucketului)". De asemenea, puteți adăuga o etichetă la bucket (în caseta "Tags(1) – optional" + "Add tag") pentru o identificare ușoară.

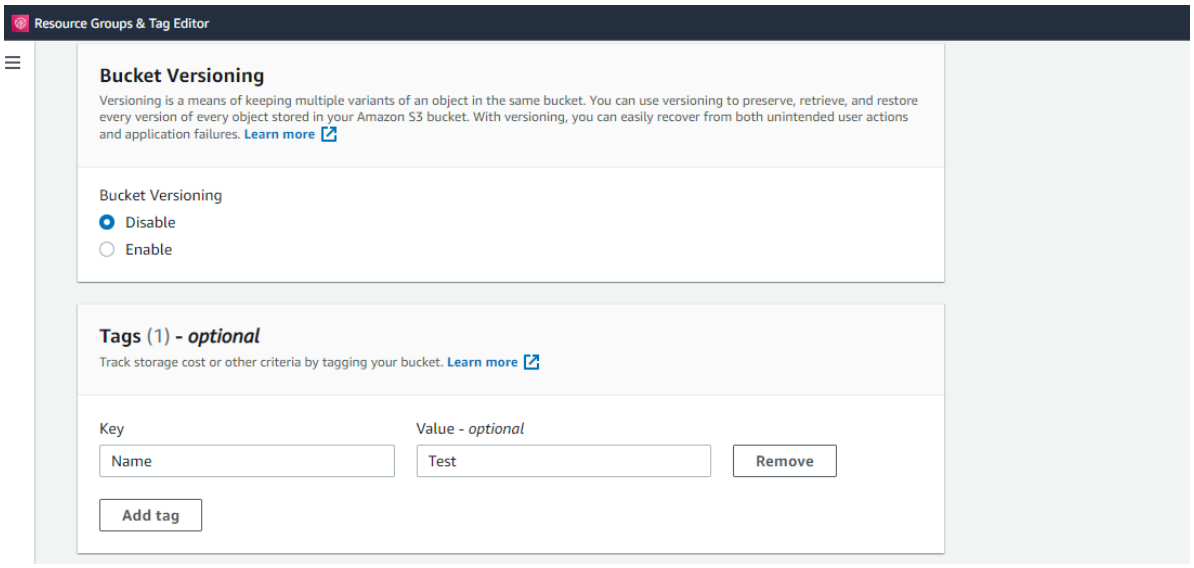

Figura 0.20. Crearea unui bucket S3 – pasul patru

În secțiunea Default encryption (Criptare implicită) faceți clic pe Enable (Activare) pentru criptarea pe server. Apoi bifaţi cheia "Amazon S3 (SSE-S3)".

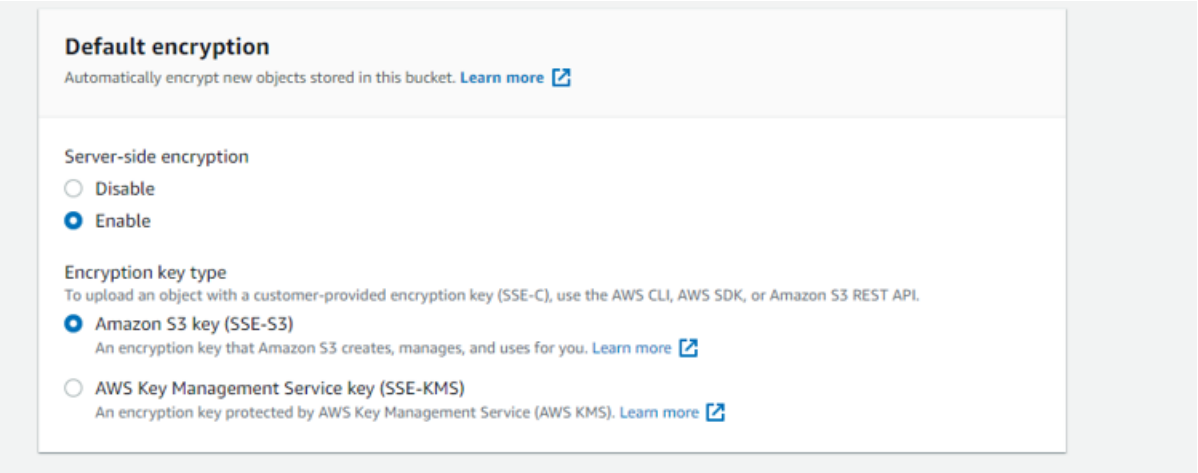

Figura 0.21. Crearea unui bucket S3 – pasul cinci

Apoi faceți clic pe Create bucket (Creare bucket).

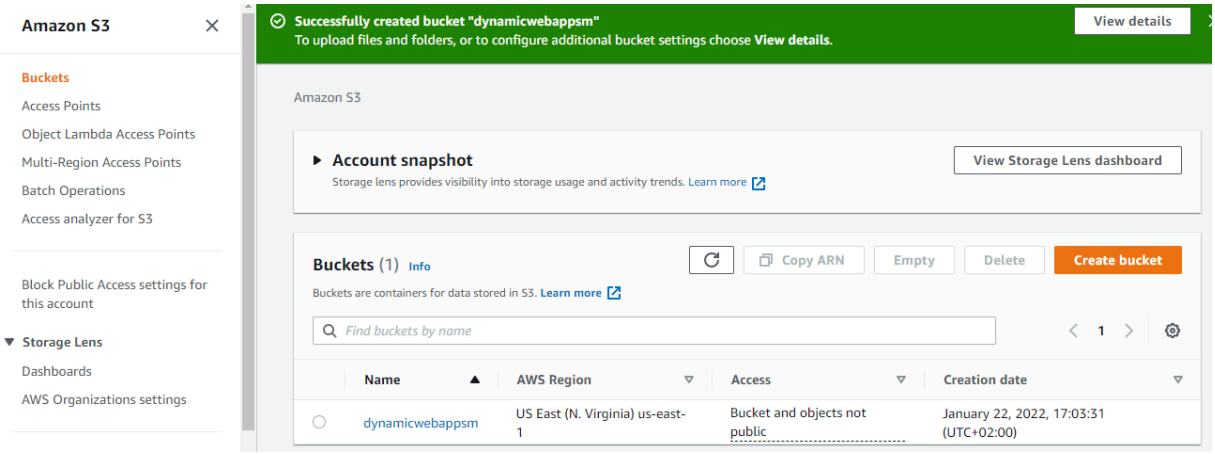

Figura 0.22. Crearea unui bucket S3 – pasul șase

Pasul 2: Încărcați fișiere web în bucket-ul S3

După crearea bucket-ului, trebuie să încărcați fișierele și folderele site-ului dvs. în el.

În dashboard (tabloul de bord) S3, faceți clic pe numele bucket-ului pe care tocmai l-ați creat “Name”.

În caseta “Objects “ (Obiecte), puteți vedea că bucketul este în prezent gol, faceți clic pe butonul Upload (Încărcare).

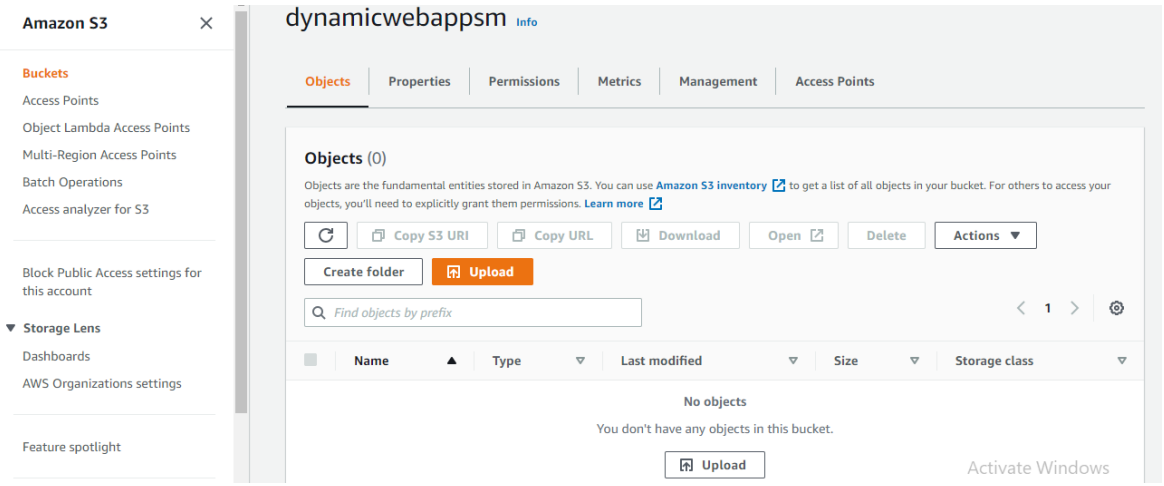

Figura 0.23. Încărcați fișiere web în bucket-ul S3 – primul pas

Acest lucru ar trebui să vă conducă la pagina Upload (Încărcare).

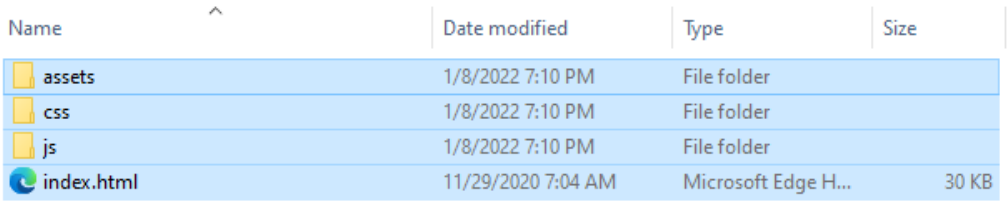

Figura 0.24. Încărcați fișiere web în bucket-ul S3 – pasul doi

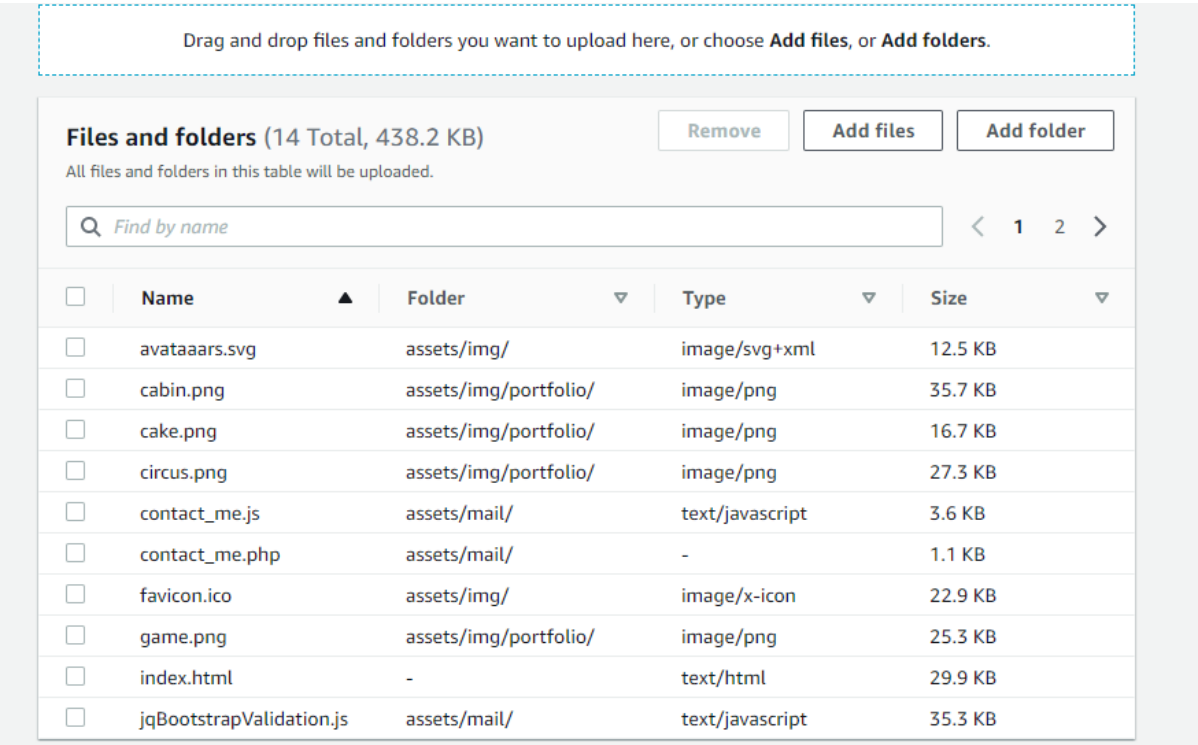

Figura 0.25. Încărcați fișiere web în bucket-ul S3 – pasul trei

După ce fișierele și folderele necesare au fost adăugate, derulați în jos și faceți clic pe Upload (Încărcare). Încărcarea ar trebui să se facă în câteva minute, în funcție de dimensiunea rețelei și a conținutului. De asemenea, vă rugăm să nu închideți fila în timp ce procesul de încărcare este în desfășurare.

Pasul 3: Creați un rol IAM

Acum, EC2 vrea să extragă cod de la S3. Deci, doriți să creați un rol IAM pentru a acorda permisiunea EC2 de a accesa S3. Pentru a face acest lucru, din meniul drop-down Servicii (Services), selectați IAM din secțiunea “Security, Identity, Compliance” (Securitate Identitate și Conformitate). Din dashboard IAM (tabloul de bord IAM), faceți clic pe “Roluri” (Roles). Apoi faceți clic pe “Create rol” (Creare rol).

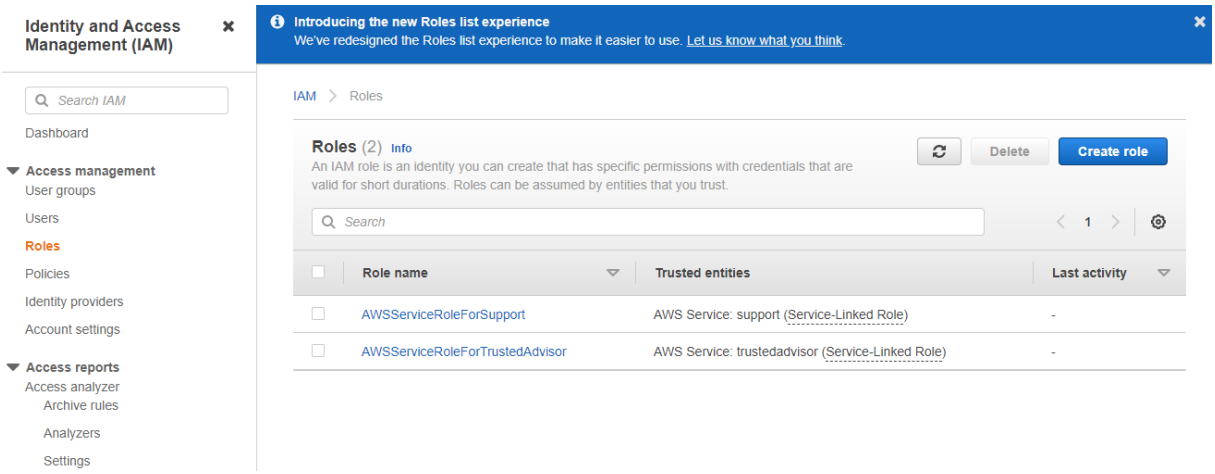

Figura 0.26. Crearea rolului IAM – primul pas

Alegeți EC2 și faceți clic pe “Next: Permissions” (Următorul: Permisiuni).

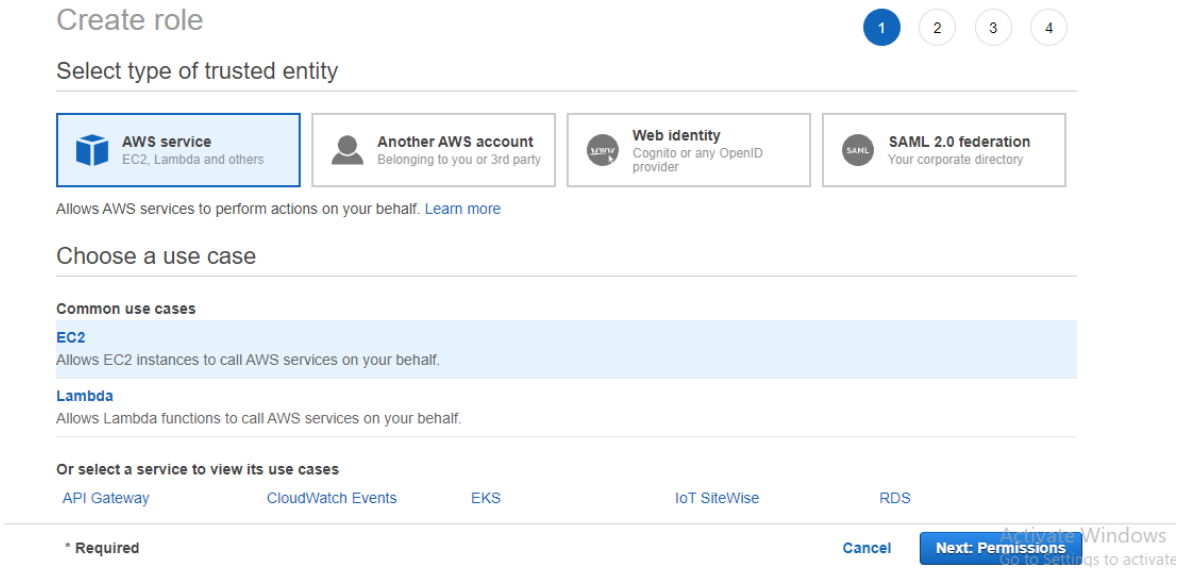

Figura 0.27. Crearea rolului IAM – pasul doi

Căutați “S3” și bifaţi “AmazonS3FullAccess”. Apoi faceți clic pe “Next: Tags” (Următorul: Etichete).

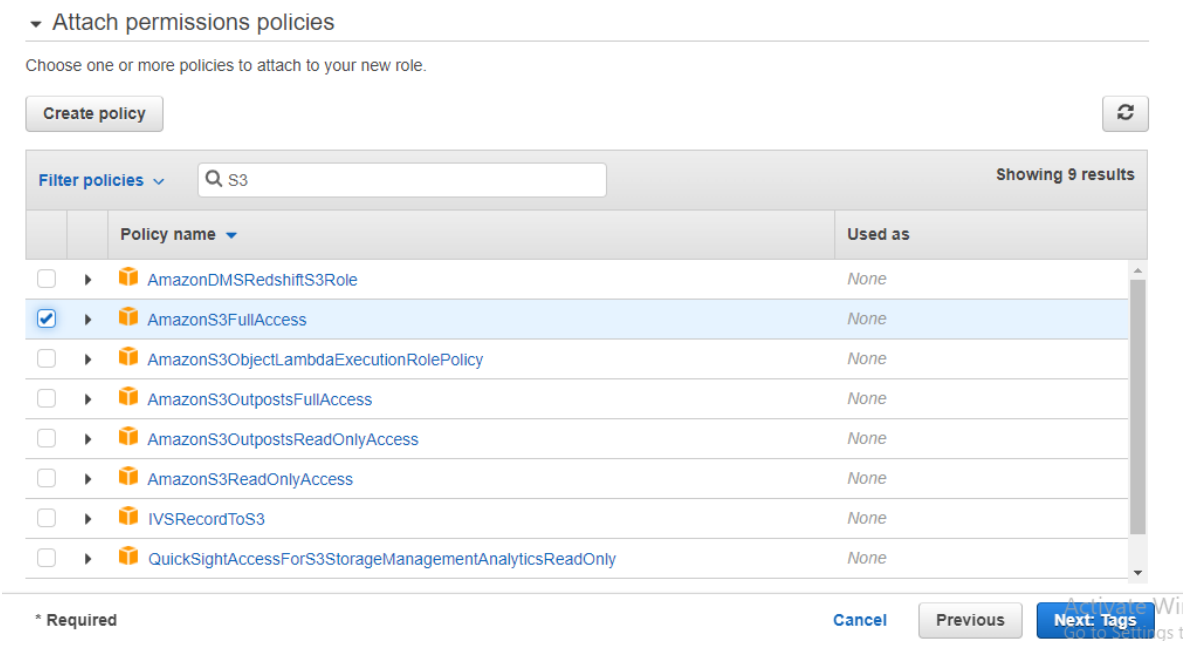

Figura 0.28. Crearea rolului IAM – pasul trei

Faceţi clic pe”Next: Review”.

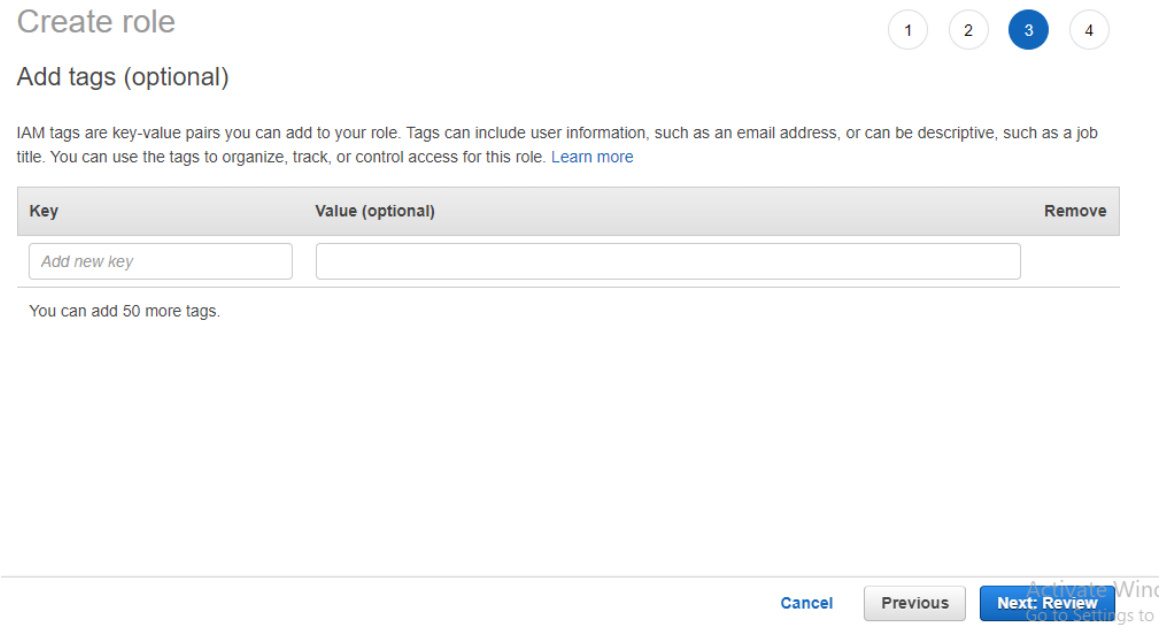

Figura 0.29. Crearea rolului IAM – pasul patru

Daţi “Role name” numele rolului şi “Role description” descrierea rolului. Apoi faceţi click pe “Create role” (Creare rol).

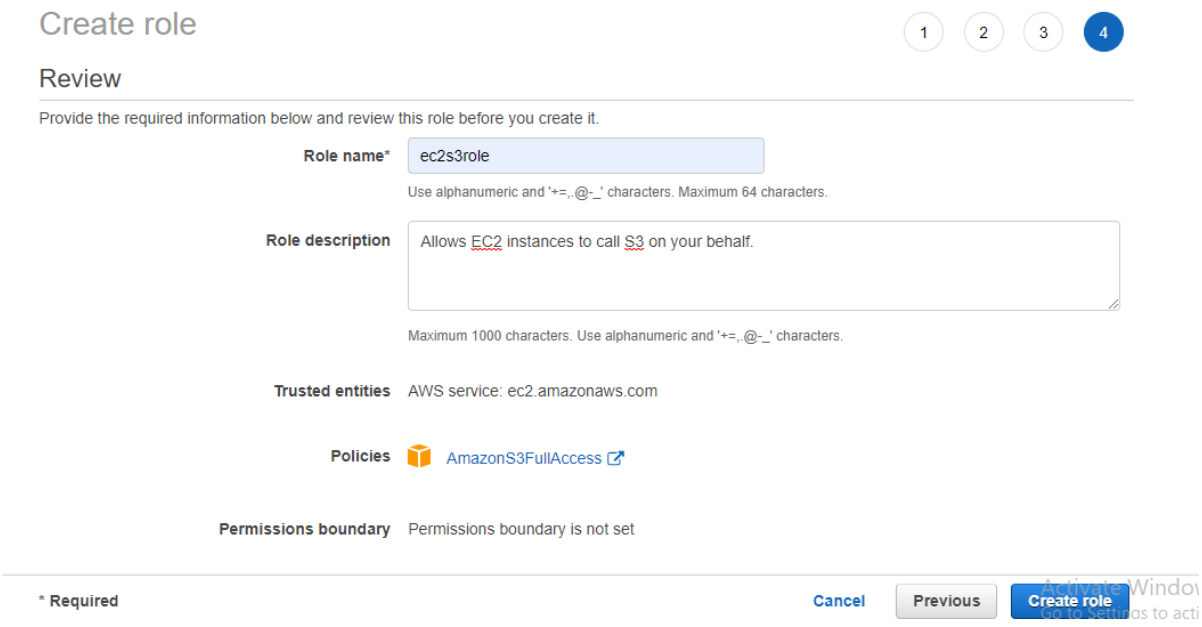

Figura 0.30. Crearea rolului IAM – pasul cinci

Acum, rolul a fost creat cu succes.

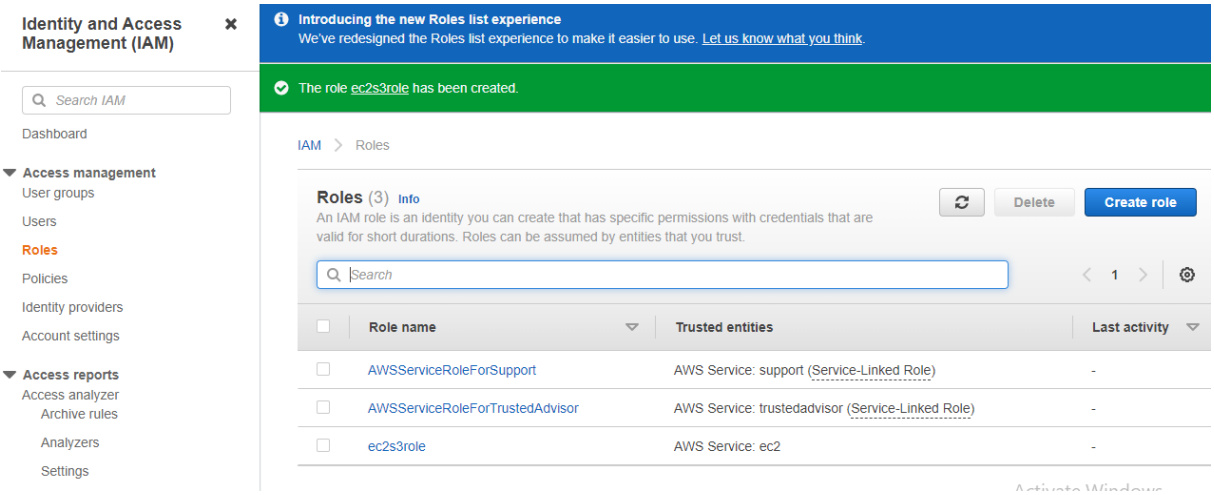

Figura 0.31. Crearea rolului IAM – pasul șase

Pasul 4: Creați o instanță EC2

Va trebui să creați o instanță EC2 pentru a instala apache (/var/www/html) și să copiați conținutul S3 în directorul html. Pentru a face acest lucru, din meniul drop-down “Services” (Servicii), selectați EC2 din secțiunea Compute. Aceasta ar trebui să afișeze tabloul de bord (dashboard) EC2. Din tabloul de bord (dashboard) EC2, faceți clic pe “Launch instance” (Lansare instanță).

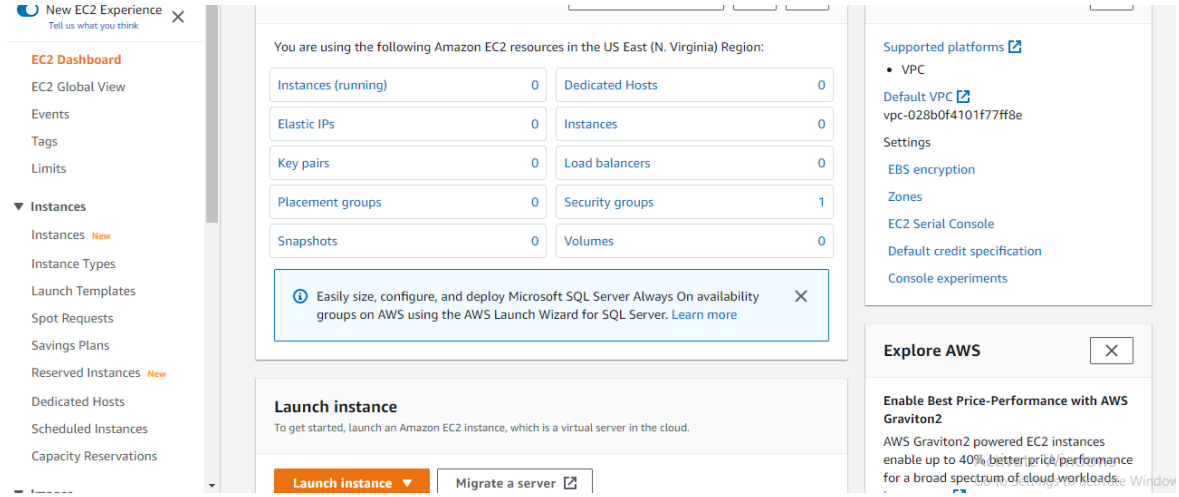

Figura 0.32. Creați o instanță EC2 – primul pas

Pentru AMI, alegeți “Quick Start” (Pornire rapidă) și faceți clic pe “Select” Selectați pentru Amazon Linux (eligibil pentru nivelul gratuit).

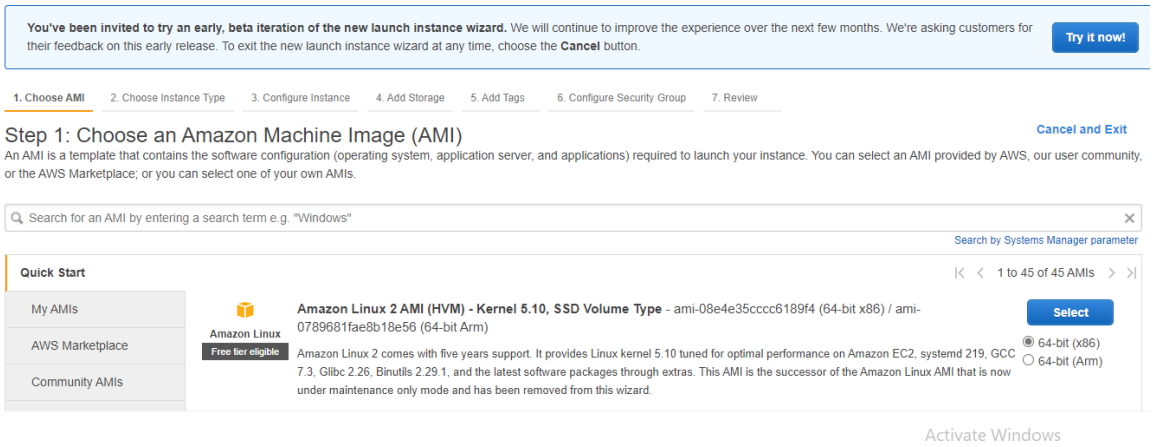

Figura 0.33. Creați o instanță EC2 – pasul doi

Pentru un tip de instanță, alegeți “t2.micro - Free tier eligible” (eligibil pentru nivelul gratuit). Și faceți clic pe Next: ConFigura Instance Details (Următorul: Configurați detaliile instanței).

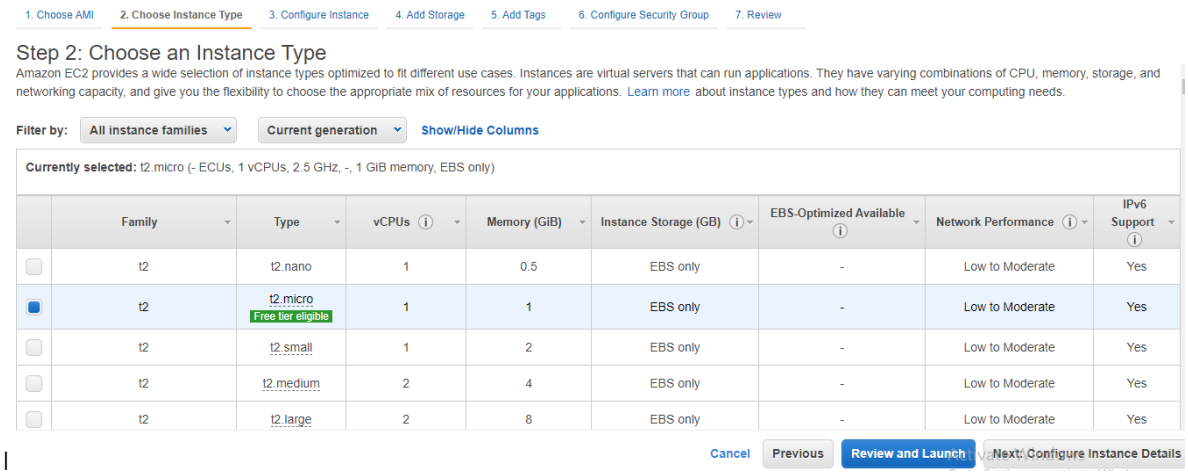

Figura 0.34. Creați o instanță EC2 – pasul trei

Determinați "1" pentru "Number of instances" (Număr de instanțe), "default vpc for Network" (vpc implicit pentru Rețea și "Default" Implicit în us-east-1a "for Subnet" (pentru Subnet).

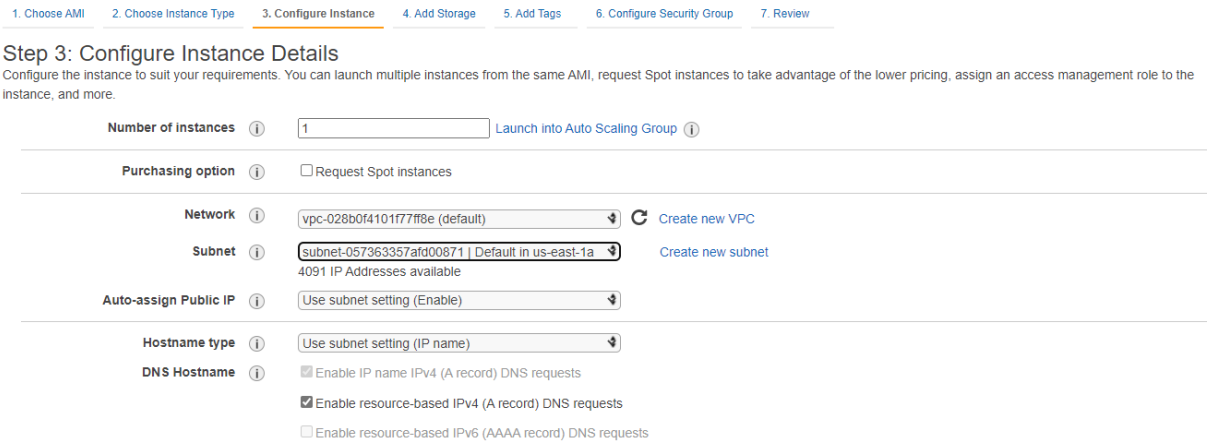

Figura 0.35. Creați o instanță EC2 – pasul patru

Alegeți "ec2s3role" sau orice ați numit pentru rolul IAM. Și "Terminate" (Terminați) pentru "Shutdown behaviour" Comportamentul de închidere. Apoi faceți clic pe "Next: Add Storage" (Următorul: Adăugați spațiu de stocare).

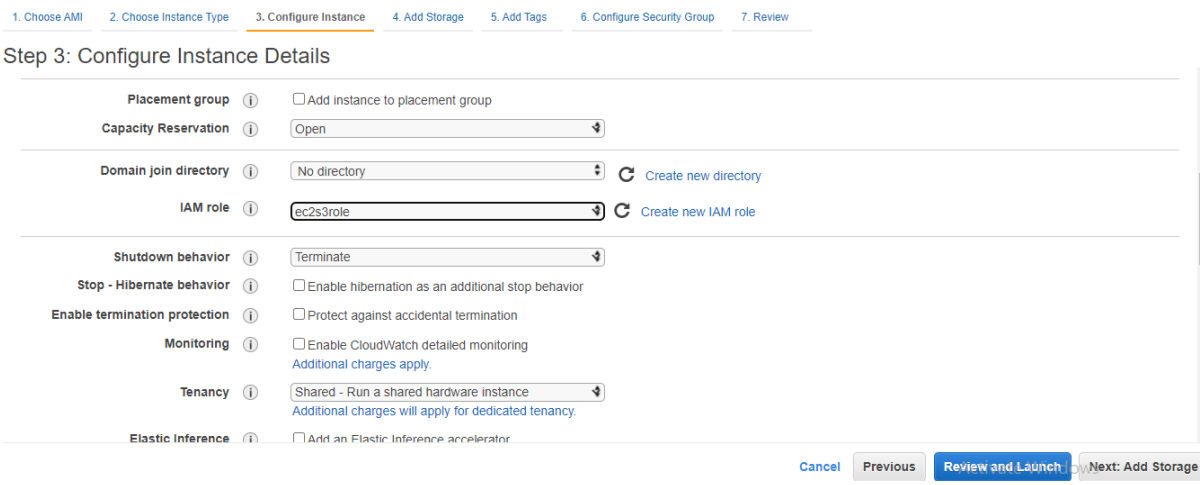

Figura 0.36. Creați o instanță EC2 – pasul cinci

Faceți clic pe “Next: Add Tags”.

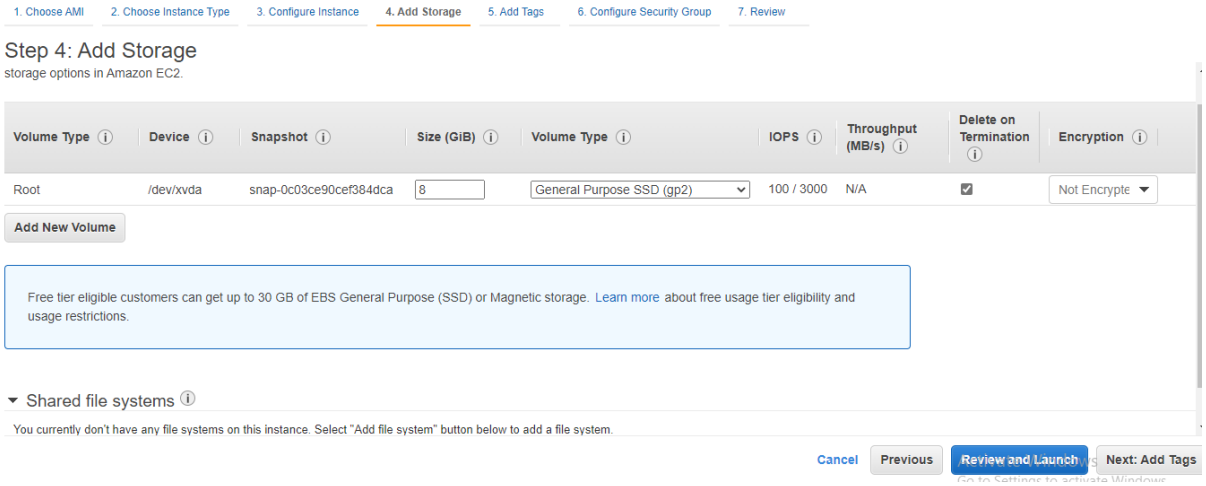

Figura 0.37. Creați o instanță EC2 – pasul şase

Puteți adăuga eticheta “Name: DynamicSite”. Apoi faceți clic pe “Next: ConFigura Security Group” (Următorul: Configurați grupul de Securitate).

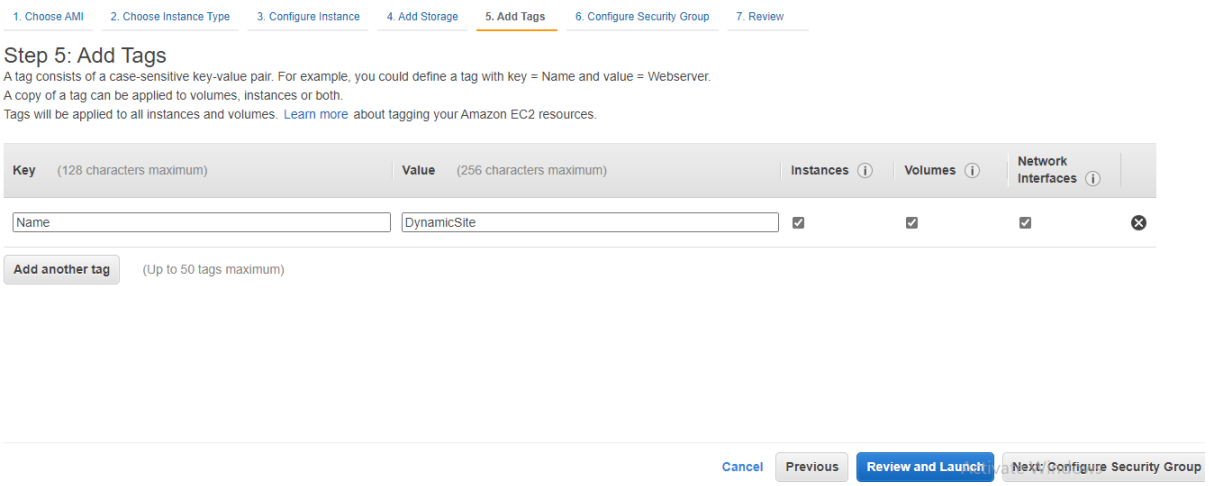

Figura 0.38 Creați o instanță EC2 – pasul șapte

Selectați "Create a new security group" (Creați un nou grup de Securitate). Dați-i Nume: "DynamicWebsiteSG" și descriere: "SG for DynamicWebApp". Pentru regula "SSH", selectați "My IP" (IP-ul meu) pentru Sursă (Source). Faceți clic pe "Add Rule" (Adăugare regulă) și selectați HTTP pentru Tip și Oriunde pentru Sursă. Ultima regulă selectați "HTTPS" pentru "Type" (Tip) și "Anywhere" (Oriunde) pentru "Source" (Sursă). Faceți clic pe "Review" (Revizuire) și "Launch" (Lansare).

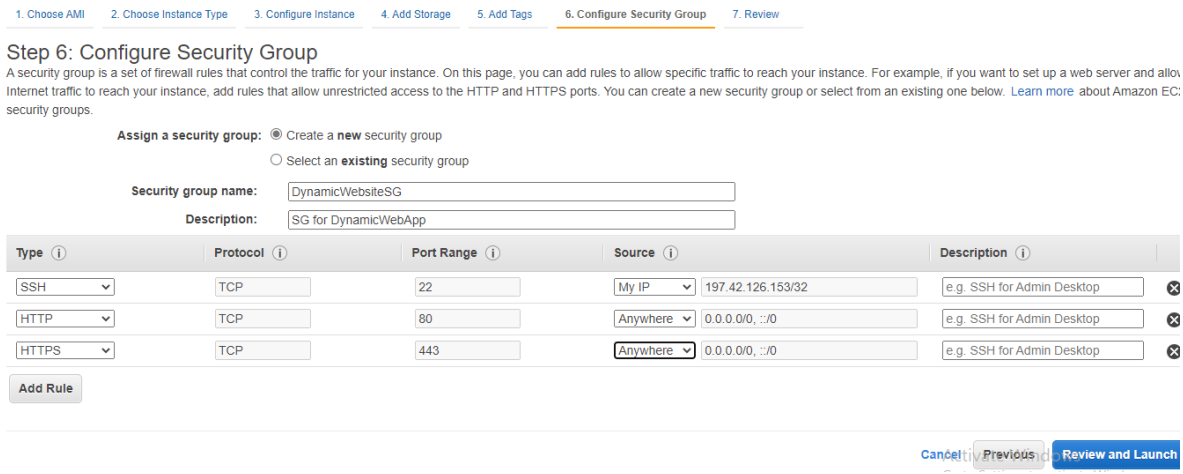

Figura 0.39. Creați o instanță EC2 – pasul opt

Faceti click pe "Launch" (Lansare).

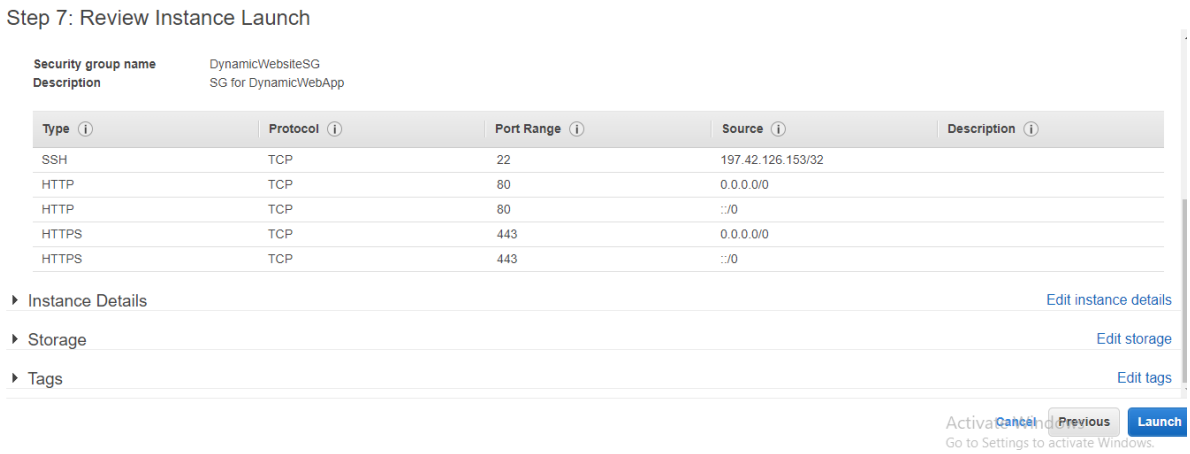

Figura 0.40. Creați o instanță EC2 – pasul nouă

Selectați “Create a new key pair” (Creați o nouă pereche de chei) și “RSA” pentru tip. Dați-i numele “WebServerKey” și faceți clic pe “Download Key Pair”. Notă: Ar trebui să descărcați cheia pentru can ssh pe EC2. Faceți clic pe “Launch Instances” (Lansare instanțe).

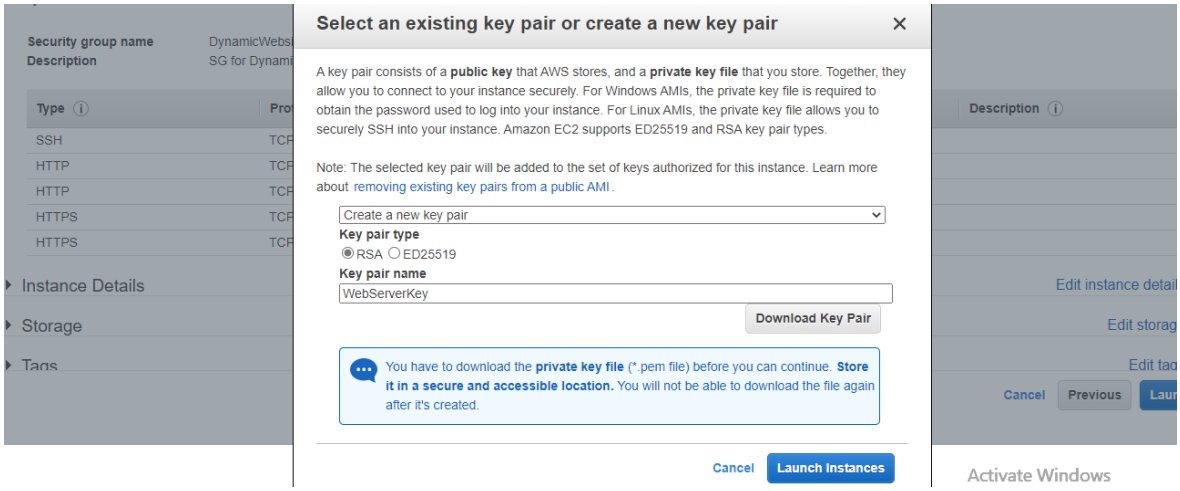

Figura 0.41. Creați o instanță EC2 – pasul zece

Acum, instanța se lansează cu succes.

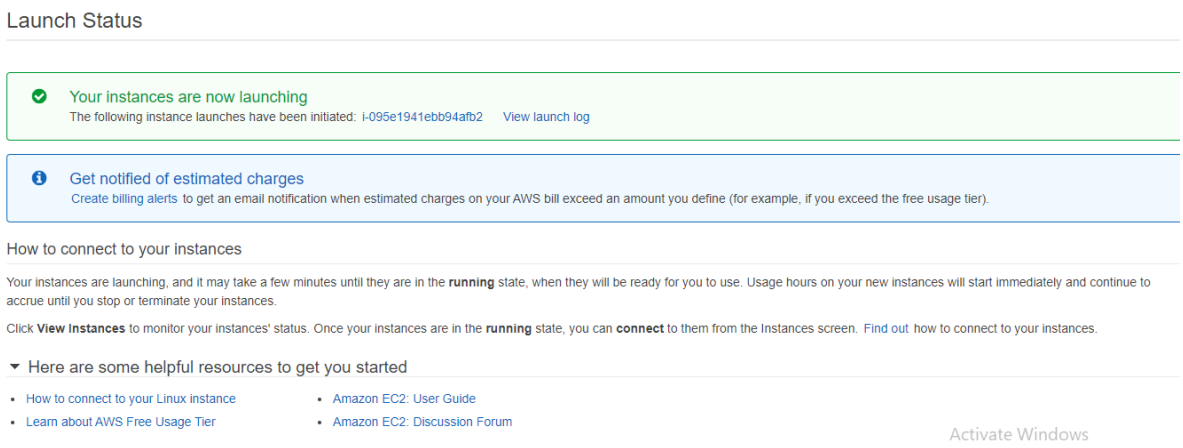

Figura 0.42. Creați o instanță EC2 – pasul unsprezece

Faceți clic pe "Review Instance" (Examinare instanță) și așteptați "Status check" (Verificarea stării) (Status check) va fi trecută de "2/2 checks passed" (2/2 verificări).

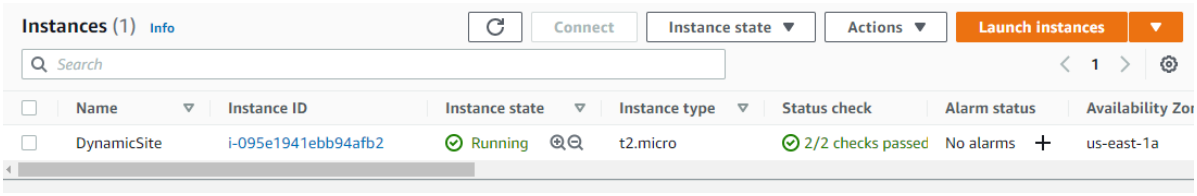

Figura 0.43. Creați o instanță EC2 – pasul unsprezece

Pasul 5: SSH cu MobaXterm

Acum, doriți să vă conectați la EC2 utilizând MobaXterm. Mai întâi ar trebui să copiați adresa IPv4 publică a instanței EC2.

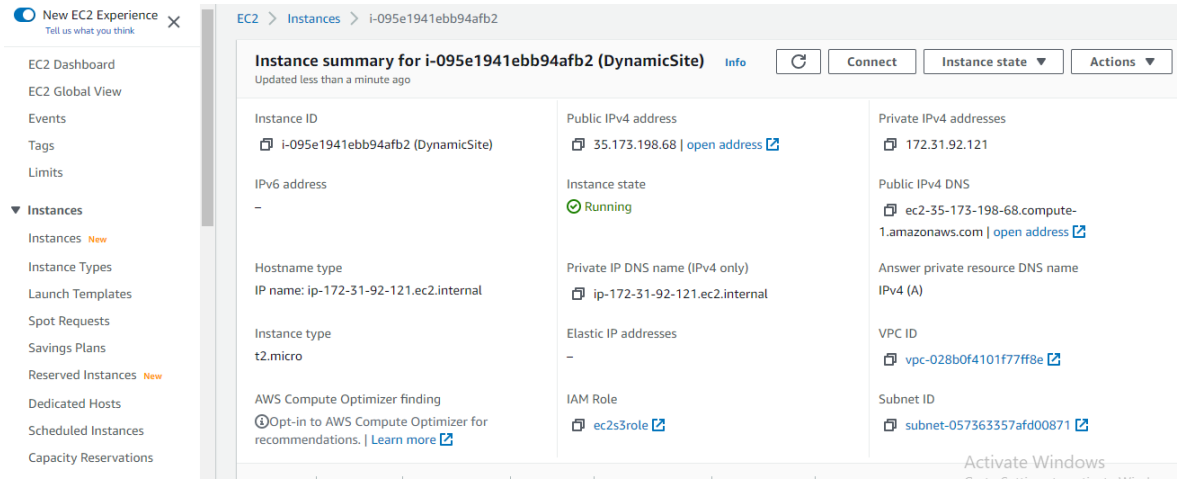

Figura 0.44. Conectarea la EC2 prin utilizarea MobaXterm - primul pas

Deschideți MobaXterm și începeți o nouă sesiune la distanță făcând clic pe Sesiune (Session).

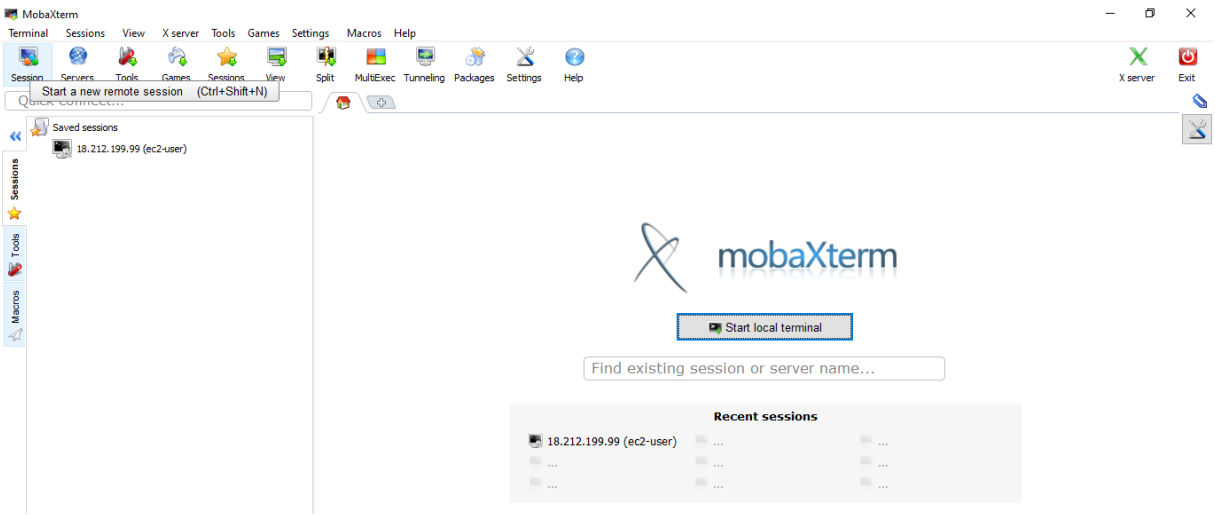

Figura 0.45. Conectarea la EC2 prin utilizarea MobaXterm – pasul doi

Faceți clic pe “SSH”. Lipiți IP-ul dvs. pentru EC2. De exemplu: (3.86.76.216). Și “ec2-user” pentru “Specify username” (Specificați numele de utilizator). Faceți clic pe “Advanced SSH settings” (Setări SSH avansate), bifați “Use private key” (Utilizați cheia private) și căutați locația cheii. Faceți clic pe OK.

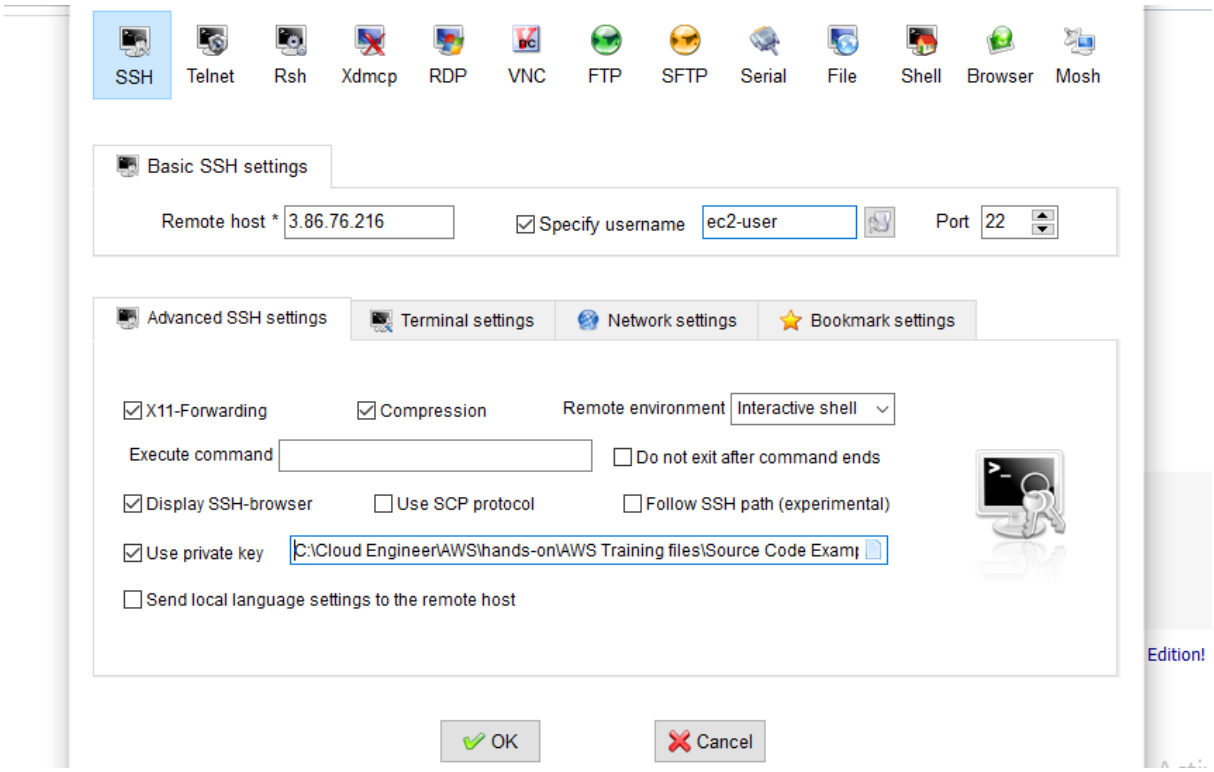

Figura 0.46. Conectarea la EC2 prin utilizarea MobaXterm – pasul trei

Acum, v-ați conectat cu succes la EC2.

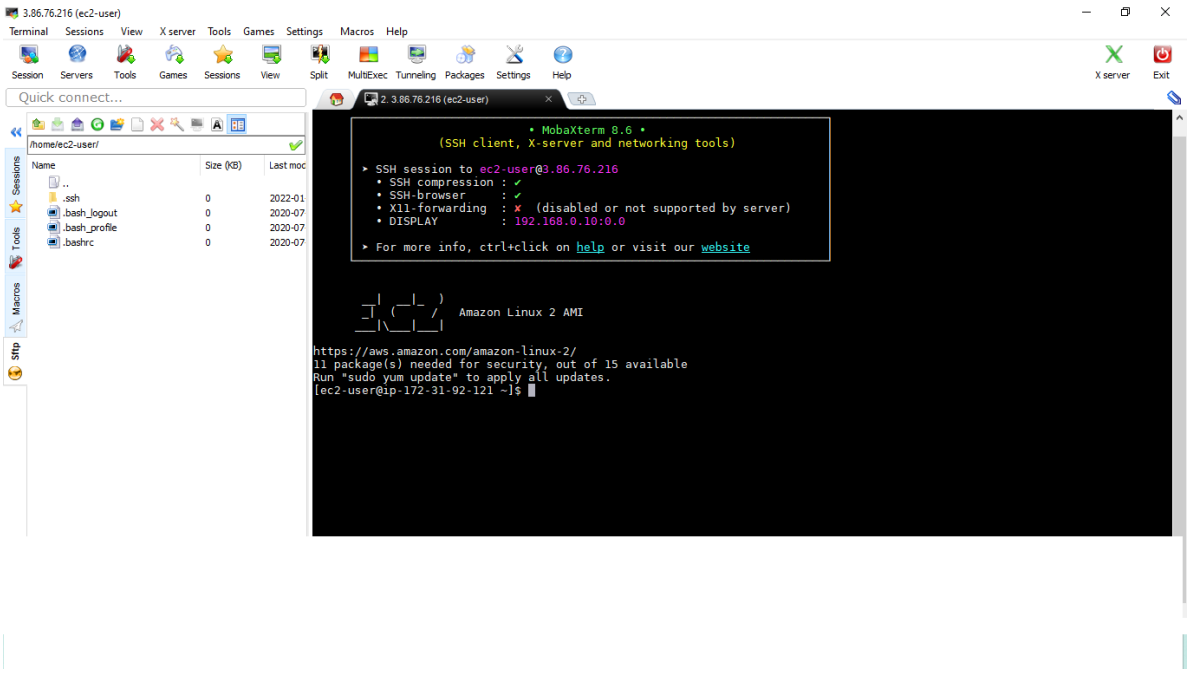

Figura 0.47. Conectarea la EC2 prin utilizarea MobaXterm – pasul patru

Pasul 6: Instalați un server web LAMP pe Amazon Linux 2

Următoarele proceduri vă ajută să instalați un server web Apache cu PHP și MariaDB. Pentru a vă asigura că toate pachetele dvs. software sunt actualizate, efectuați o actualizare rapidă a software-ului pe instanță.

sudo yum update -y

Instalați depozitele "lamp-mariadb10.2-php7.2" și "php7.2" Amazon Linux Extras pentru a obține cele mai recente versiuni ale pachetelor LAMP MariaDB și PHP pentru Amazon Linux 2.

sudo amazon- linux -extras install -y lamp-mariadb10.2-php7.2 php7.2

Acum, puteți instala serverul web Apache, MariaDB și pachetele software PHP.

sudo yum install -y httpd mariadb -server

Porniți serverul web Apache.

sudo systemctl start httpd

Utilizați comanda systemctl pentru a configura serverul web Apache să pornească la fiecare pornire (boot-are) a sistemului.

sudo systemctl enable httpd

Puteți verifica dacă "httpd" este "on" rulare pornită

sudo systemctl este activat httpd

Acum, doriți să copiați conținutul site-ului web din S3 în directorul / var /www/html în EC2. Asigurați-vă că copiați numele bucket-ului S3.

sudo aws s3 cp s3://dynamicwebappsm --region us-east-1 / var /www/html/ --recursive

Pentru a verifica dacă conținutul este copiat în / var /www/ html.

cd/var /www/html

Copiați DNS IPv4 public și inserați-l într-o filă nouă.

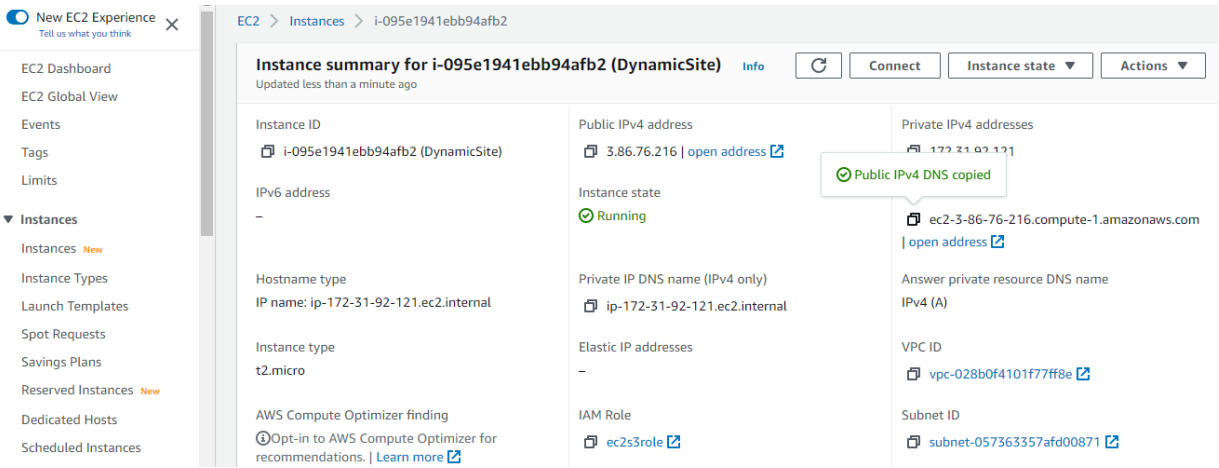

Figura 0.48. Instalarea unui server web LAMP pe Amazon Linux 2

Felicitări, ați implementat cu succes un site web dinamic pe EC2.

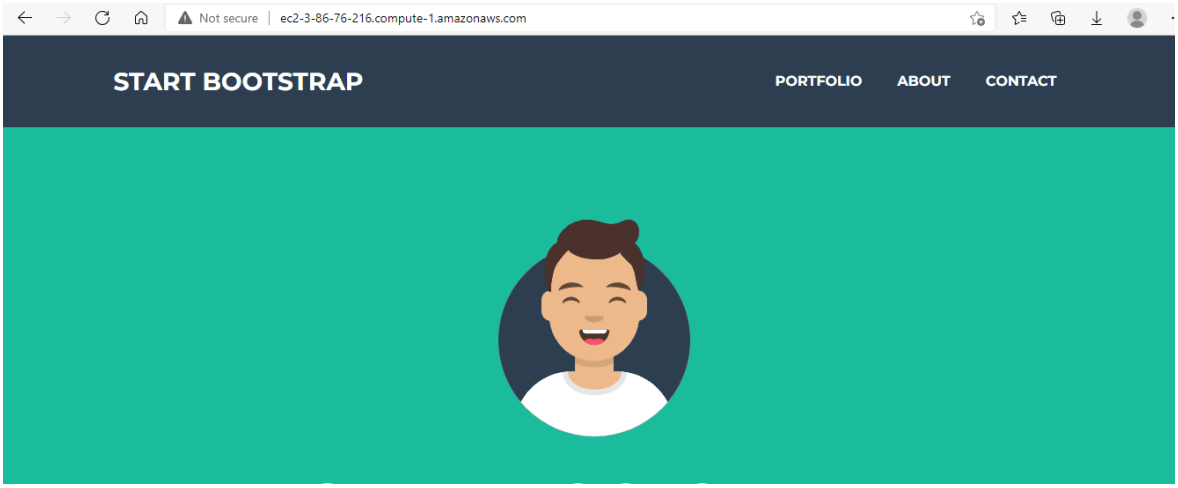

Figura 0.49. Implementarea cu succes a unui site web dinamic pe EC2

Caz de utilizare: găzduiește un site web static folosind AWS (sau alte cloud-uri)

Ghid pas cu pas

Configurații de bază

- Accesați consola S3 și creați un nou bucket cu setările implicite.
- Accesați „properties" proprietățile bucket-ului dvs. și alegeți opțiunea „Găzduire statică a site-ului web" (Static website hosting).
- Activați opțiunea „Use this bucket to host a website„ (Utilizați acest bucket pentru a găzdui un site web).
- Furnizați numele codului HTML care va fi afișat ca pagină de pornire și fișierul HTML care va fi afișat în cazul în care apare o eroare pe site-ul dvs.

Opțional, furnizați reguli de redirecționare dacă doriți să direcționați cererile în mod condiționat în funcție de nume specifice de chei de obiect, prefixe din cerere sau coduri de răspuns către un alt obiect din acelaş bucket sau adresă URL externă.

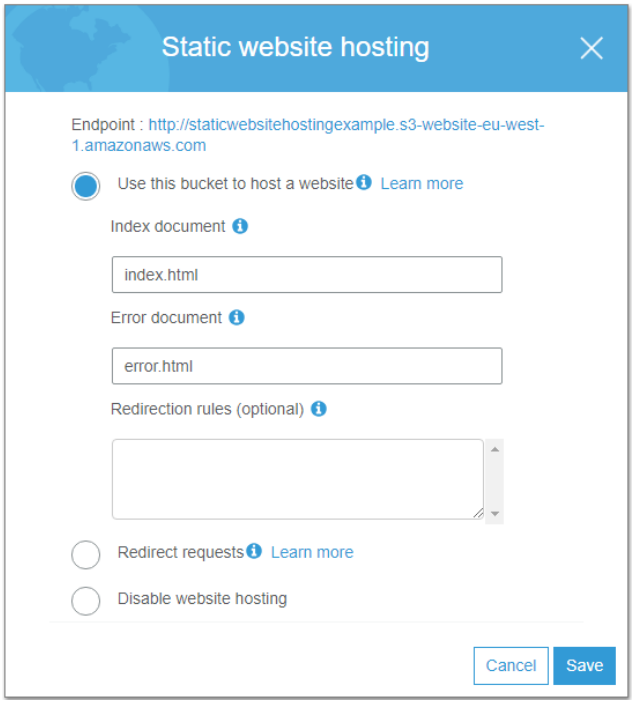

Figura 0.50. Găzduiește un site web static utilizând AWS – primul pas

Acum, accesați secțiunea "Permissions" Permisiuni a compartimentului dvs. și adăugați următoarele în secțiunea "Bucket Policy" (Politica Bucket-ului):

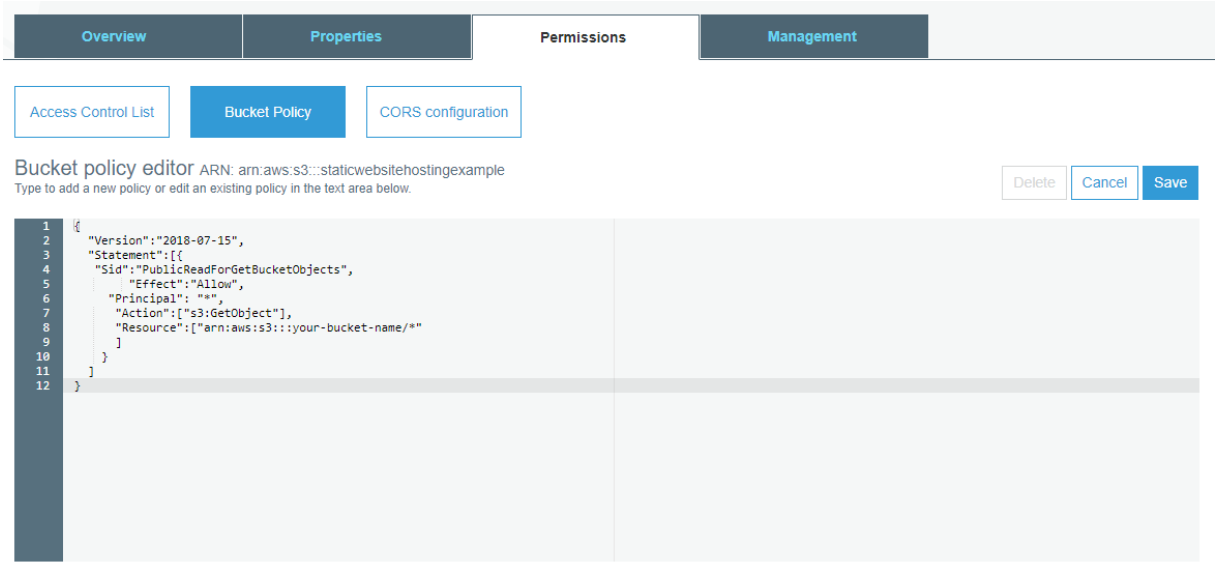

Figura 0.51. Găzduiește un site web static utilizând AWS

Schimbă "*your-bucket-name*" cu numele bucket-ului tău.

Pentru a permite site-ului dvs. static S3 să răspundă la solicitări precum GET și POST care provin de la o aplicație externă găzduită pe un anumit domeniu, ar trebui să configurați CORS în setările compartimentului. Pentru a face acest lucru, adăugați următoarele în secțiunea de configurare CORS din Permisiuni (:Permissions):

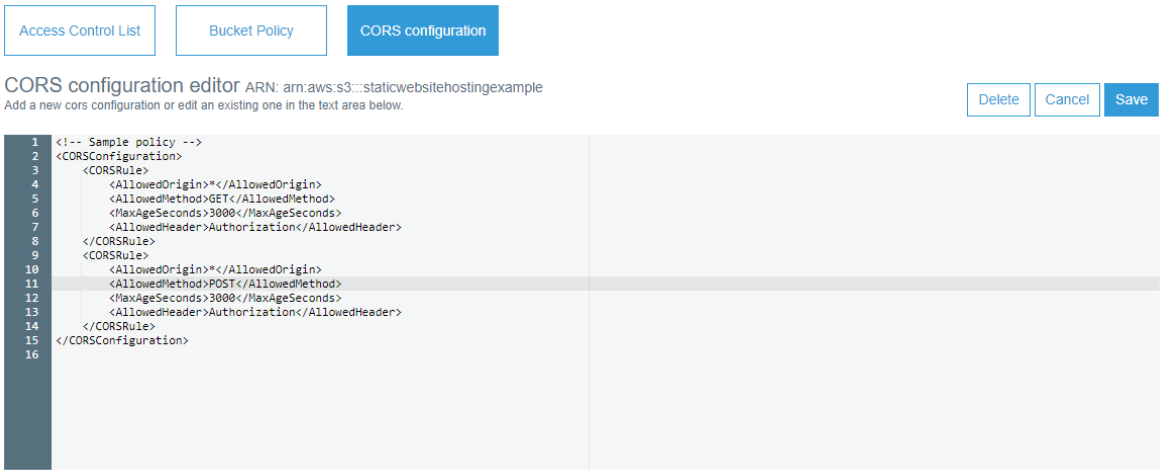

Figura 0.52. Găzduiește un site web static utilizând AWS – pasul doi

Încărcați codul dvs. Pentru acest tutorial, creați două fișiere HTML simple cu numele index.html și error.html și încărcați-le într-un bucket.

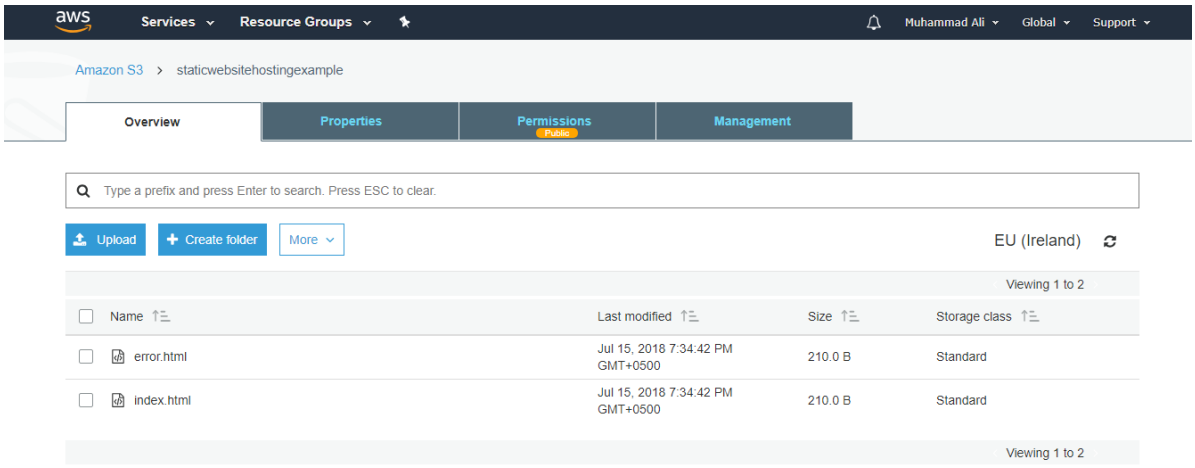

Figura 0.53. Găzduiește un site web static utilizând AWS – pasul trei

Pentru a lansa și a testa site-ul, punctul final poate fi preluat din Proprietăți (Proprietes) > Găzduire statică a site-ului web (Static website hosting).

Îmbogățiți-vă site-ul web prin adăugarea unui comportament dinamic

Puteți folosi o combinație dintre HTML5 și CSS3 pentru a vă îmbogăți grafic site-ul. De asemenea, puteți utiliza jQuery Ajax pentru a apela un API (microserviciu) și pentru a prelua dinamic date dintr-o sursă de date și pentru a le afișa pe site-ul dvs. web. În mod similar, prin invocarea punctelor finale API folosind Ajax, puteți stoca orice tip de date ale utilizatorului înapoi în sursa dvs. de date, ca la orice altă aplicație web. Dacă cerința dvs. este să utilizați AWS numai pentru toate dvs. de dezvoltare, puteți utiliza o combinație de API Gateway și Lambda pentru a construi API-uri, un tutorial pentru care poate fi găsit aici.

Setări CORS în punctele finale API Gateway

Este important să rețineți că atunci când dezvoltați API-uri (microservicii) folosind un API Gateway (poarta de acces API) și Lambda, asigurați-vă că faceți următoarele:

Activați CORS în poarta de acces API (API Gateway) în momentul creării unei noi resurse.

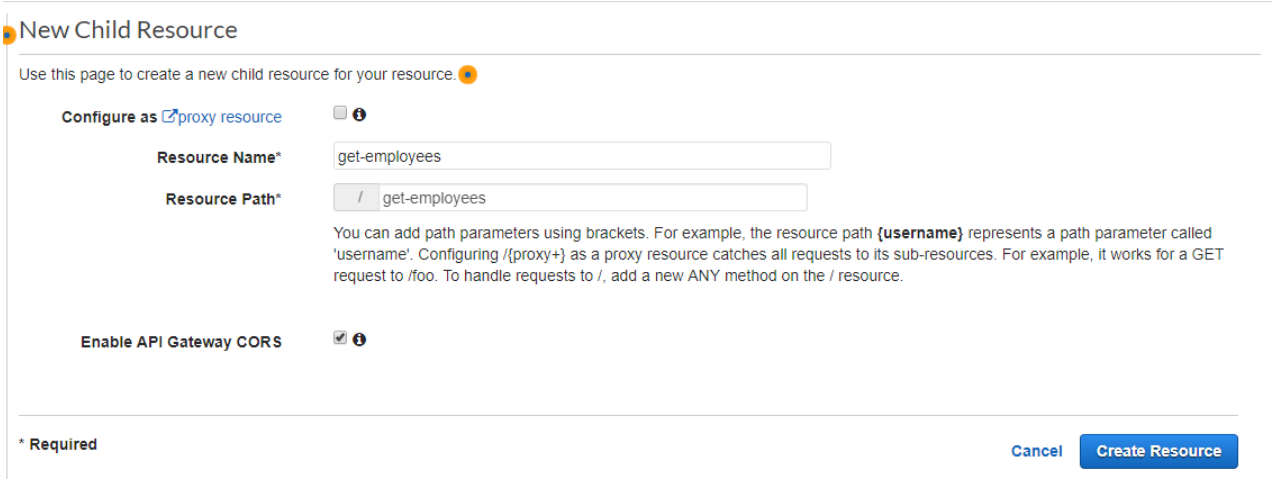

Figura 0.54. Găzduiește un site web static utilizând AWS – pasul patru

Când scrieți funcția lambda (pe care o veți integra cu punctul final API Gateway pentru a oferi funcționalitate microserviciului), asigurați-vă că adăugați un parametru suplimentar în antetul răspunsului cu numele Access-Control-Allow-Origin cu valoarea „*”