

**UNIVERSITATEA „BABEȘ-BOLYAI”
FACULTATEA DE MATEMATICĂ ȘI INFORMATICĂ
SPECIALIZAREA SISTEME DISTRIBUITE ÎN INTERNET**

Lucrare de disertație

MONITORIZAREA PROGRAMATICĂ A RESURSELOR AZURE

Coordonatori științifici
Lect. **Sergiu-Adrian Dărbant**

Absolvent
Bogdana Cărașan

**Cluj-Napoca
2018**

1 INTRODUCERE

1.1 INTRODUCERE

Microsoft Azure, o soluție cloud consacrată deja pe piața cloud aduce inovații și îmbunătățiri vizibile de la lună la lună. Acoperând deja partea de securitate, baze de date, aplicații web, infrastructuri micro-services, servicii de gestionare a logurilor și multe altele, această lucrare își propune să ofere o prezentare și asupra serviciilor puse la dispoziție de Azure pentru monitorizarea acestor resurse mai înainte amintite.

Prin monitorizare înțelegem urmărirea integrității, disponibilității, performanței, timpului de răspuns, evidența situațiilor critice, pe scurt, buna funcționare a unui serviciu de care depinde aplicația ta.

Azure dispune de mai multe servicii de monitorizare, fiecare cu un anumit rol și anumite funcționalități, apărute în urma cerințelor pieței. Aceste servicii colectează date așa zis numite metrice, pe care le stochează o anumită perioadă de timp și care sunt disponibile spre a fi citite sau procesate prin diferite unelte puse la dispoziție de ei, sau simple API-uri.

Această lucrare relatează noțiuni generale despre resursele Azure care vor fi monitorizate în aplicația prezentată, dar desigur și despre serviciile de monitorizare care pot fi folosite pentru colectarea datelor.

Capitolul 1 conține date introductive ale acestei lucrări, precum cuprins, abstract și o scurtă introducere.

Capitolul 2 prezintă o prezentare foarte scurtă asupra conceptului de cloud computing și ceea ce îl definește.

Capitolul 3 descrie strategia cloud oferită de Microsoft, Windows Azure împreună cu cele mai populare servicii oferite de aceștia. Toate serviciile Azure care sunt folosite spre a fi monitorizate în aplicația descrisă din capitolul 5, sunt descrise în prealabil în acest capitol.

Cel mai important, sunt descrise serviciile de monitorizare disponibile în acest moment în Azure, cu scopul de a lămuri funcționalitățile generale ale acestora.

Capitolul 4 relatează în plus față de capitolul 3 detalii despre datele furnizate de aceste servicii de monitorizare pe care le numim metrici, caracteristicile lor și modurile de interogare a acestora.

Capitolul 5 este despre implementarea aplicației, structura acesteia împreună cu explicații, oferite și vizual prin intermediul diagramelor dar și capturilor de ecran ce reprezintă interfața grafică cu utilizatorul. Sunt explicate desigur și cazurile de utilizare și tehnologiile folosite.

Capitolul 6 cuprinde concluzii aduse serviciilor de monitorizare. Referințele folosite pentru elaborarea lucrării sunt înșirate în capitolul 7.

1.2 CUPRINS

1	Introducere.....	2
1.1	Introducere	2
1.2	Cuprins	4
1.3	Abstract	6
2	Cloud Computing	7
2.1	Informații generale	7
2.1.1	Origine concept.....	7
2.1.2	Modelul NIST	8
2.1.3	Beneficii și provocări.....	9
3	Microsoft Windows Azure	11
3.1	Introducere	11
3.2	Tipuri de resurse.....	12
3.2.1	Azure Active Directory.....	13
3.2.2	Azure Virtual Machines	13
3.2.3	Azure Websites	13
3.2.4	Event Hub	13
3.2.5	Azure Storage.....	14
3.3	Serviciile Azure de monitorizare.....	15
3.3.1	Serviciile Shared Capabilities	16
3.3.2	Core Monitoring.....	17
3.3.3	Serviciile Deep Monitoring.....	18
3.3.4	Serviciile Deep Infrastructure Monitoring.....	19
4	Metrici	21
4.1	Prezentare generală	21
4.2	Metrici de bază.....	22
4.3	Metrici multi-dimensionali.....	23
4.4	Interogarea metricilor	23
4.4.1	Azure Portal	23
4.4.2	Azure storage	24

4.4.3	Azure CLI & Powershell	25
4.4.4	REST API	25
5	Dezvoltarea aplicativă	26
5.1	Prezentare	26
5.2	Tehnologii	26
5.3	Proiectare.....	27
5.3.1	Cazuri de utilizare	27
5.3.2	Componentele aplicației.....	28
5.3.3	Diagrama de arhitectură.....	29
5.4	Colectarea metricilor	29
6	Manual de utilizare	30
7	Concluzie	32
8	Bibliografie.....	33

1.3 ABSTRACT

More than a few years ago Cloud computing was a relative new concept, with the potential to transform the entire IT industry through its way of providing scalable hardware and software resources. Nowadays we have so many types of services that a cloud computing solution has to offer that it has become interesting looking into maybe not such a necessary, at-first look, feature but actually it is a very important one, monitoring.

By monitoring we should understand the reliability, availability, evidence of critical issues, premonition of possible problems, abnormalities in usage and performance of the application. In cloud, a application will consist of several of hosted resources, so a monitoring system or strategy is needed for the application's services health and better performance.

This research paper plans on focusing and discovering the monitoring services capabilities of a cloud solution like Windows Azure. Azure has made a long way in developing consistent services, catching up with what's vogue on the market and it made no exception in developing strategies for monitoring the performance of the services that it has to offer.

Other research papers or books on this matter were to be not found and all the information around interrogating metrics is based on Azure's official documentation.

Chapter 1 contains introductory information of the thesis, like summary, this abstract and a short introduction. Chapter 2 presents generally the concept of cloud computing while chapter 3 digs more into the Azure's cloud monitoring system strategy along with the most popular services provided by their cloud platform Windows Azure that will be used on monitoring demonstration.

Chapter 4 offers an overview of the metrics, their characteristics and ways of interrogation, on chapter 5 we continue with presenting the software engineering process on which the application was designed through diagrams with the app user guide and explanations of the application flow and the functionalities that it has. Chapter 6 contains conclusions of the concept of cloud computing and the references used in application are enumerated in chapter 7.

This work is the result of my own activity. I have neither given nor received unauthorized assistance on this work.

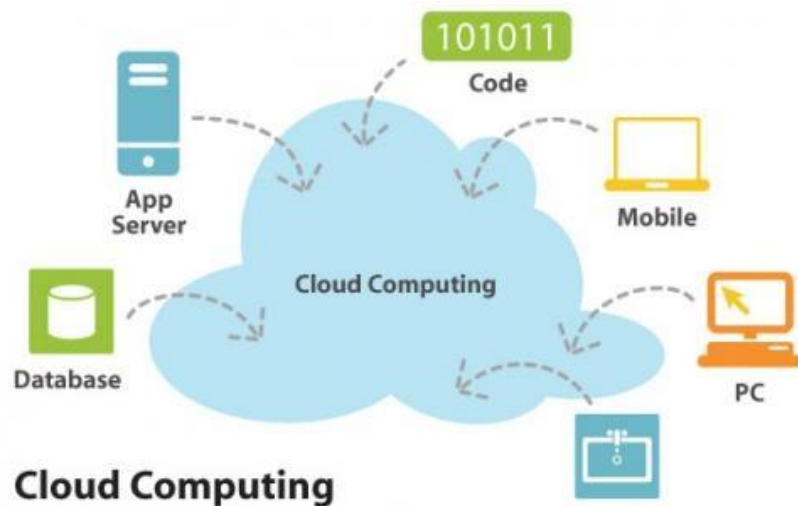
2 CLOUD COMPUTING

2.1 INFORMAȚII GENERALE

2.1.1 Origine concept

Cloud computing ca și concept reprezintă o infrastructură virtuală care se poate alcătui din resurse atât hardware cât și software, invizibilă clientului, de unde derivă și termenul de cloud (“nor”). de gestionare a unei afaceri și aprovizionare de servicii. Folosind o conexiune la Internet, un utilizator, localizat oriunde pe glob, poate accesa o resursă găzduită în *cloud*, localizată în alte puncte de pe planetă.

Serviciile cloud oferite se alcătuie în mare parte din echipamente de calcul, spațiu de stocare, aplicații, licențe necesare, servere și tot ce ține de administrarea, climatizarea, întreținerea acestora cât și angajarea unui personal tehnic specializat care se ocupă de mentenanță.



Figură 2.1 Cloud Computing [22]

Multe companii mici care înainte nu își permiteau toate aceste cheltuieli pot apela la un furnizor care oferă aceste servicii, de obicei pe baza modelului de plată *pay-as-you-go* (plătești cât consumi). Acum câțiva ani comunitatea IT era sceptică în legătură cu ideea de cloud, în ziua de azi, tot mai multe companii încep să își migreze aplicațiile în cloud iar programarea în cloud este tot mai căutată. Astfel și numărul de companii ofertante de soluții cloud crește, sau aduc constant inovații și actualizări serviciilor pe care le furnizează. [1]

2.1.2 Modelul NIST

2.1.2.1 Definiția NIST

Institutul Național pentru Standarde și Tehnologie din Statele Unite a dat următoarea definiție: „Cloud computing este un model care permite accesul la o rețea formată din resurse de calcul configurabile (ex: rețele, servere, spațiu de stocare, aplicații și servicii) într-un mod omniprezent, convenabil, disponibil la cerere, resurse care pot fi livrate rapid și cu un minim efort de administrare sau interacțiune umană”. [2]

2.1.2.2 Caracteristicile esențiale NIST

- **Servicii la cerere.** Un consumator poate în orice moment, aproape instant, să-și aprovizioneze în mod independent orice resursă de calcul necesară fără nevoia de interacțiune umană cu furnizorul. Având această libertate există posibilitatea ca clientul, fără de cunoștință, să-și depășească limita de cost permisă. Astfel, procurorii de servicii colectează și măsoară cerințele consumatorilor ca de exemplu Amazon, folosindu-se de sistemul de alertă propriu, CloudWatch. [3]
- **Acces în bandă largă.** De pe orice fel de dispozitiv (telefoane mobile, tablete, laptop-uri, PC-uri ș.a.) clientul poate accesa de la distanță, fără nevoia de a cunoaște locația destinație, resursele de care are nevoie, prin intermediul Internet-ului. [3]
- **Resurse comune.** Un furnizor de servicii cloud trebuie să servească mai mulți clienți, simultan. Aplicația fiecăruia este consumatoare de resurse virtuale și fizice, alocate dinamic, care se asignează fiecăreia în parte într-o anumită ordine, de aceea resursele oferite de cloud pot fi considerate ca fiind folosite la comun, deoarece sunt redistribuite la fiecare pas în funcție de cererea clienților. [3, 5]
- **Flexibilitate (elasticitate).** Această caracteristică se referă la cât de rapid, în lipsă de intervenție umană, se pot scala resursele, în funcție de cât cere consumatorul. Pentru el resursele oferite de cloud apar ca “fiind nelimitate și pot fi cumpărate în orice cantitate și oricând.” [3, 5]
- **Sistem de măsurare.** Un astfel de sistem de monitorizare este folositor atât clientului, cât și furnizorului, pentru a ține evidența resurselor utilizate. Prețul acestora este calculat în funcție de tipul fiecăruia (stocare, procesare, lărgime de bandă) și comunicat consumatorului pentru o cât mai mare transparență. [4, 3]

2.1.2.3 Modele și tipuri de servicii cloud

Un utilizator sau o aplicație poate utiliza cloud prin serviciile disponibile oferite de către acesta. Din punct de vedere abstract, putem privi cloud computing compus din: *Infrastructure as a Service* (IaaS), *Platform as a Service* (PaaS) și *Software as a Service* (SaaS), aplicabile pe orice tip de cloud. „Aceste nivele de abstractizare pot de asemenea fi vizionate sub formă de arhitectură pe straturi unde serviciile de pe nivel mai înalt sunt compuse din serviciile de pe straturile inferioare”. [4, 7]

Companii ca Google, Amazon și Microsoft sunt furnizori specializați de servicii cloud care asigură și actualizări de software către publicul larg. Acest tip de cloud îl întâlnim sub denumirea de **Public Cloud**. Cel mai mare risc la alegerea acestui tip o reprezintă securitatea, dar ca avantaj, această soluție este cea mai puțin costisitoare. [4, 6]

2.1.3 Beneficii și provocări

2.1.3.1 Avantaje

❖ Costuri infime

Dezvoltarea și mentenanța unei infrastructuri proprii implică o investiție mare și se face cu riscul apariției unor tehnologii noi mai bune sau neutilizarea resurselor la capacitatea maximă în care s-a investit. Furnizorii cloud se ocupă de întreținerea acestor sisteme IT, consumatorii cer doar resursele de care au nevoie, astfel ei plătesc doar cât consumă.

❖ Implementare rapidă

În urma încheierii unui contract cu un furnizor de soluții cloud, companiei îi rămâne de implementat doar partea de structură personalizată după nevoile ei, și în funcție de furnizorul ales, folosindu-se de instrumentele de implementare a acestuia.

❖ Elasticitate

Compania ofertantă de soluții cloud se angajează ca structura oferită de ei să poată fi mărită sau micșorată la cererea utilizatorului.

❖ Siguranță

Asemenea, o altă responsabilitate a furnizorului este siguranța datelor clientului, lucru pe care îl obține prin replicarea acestora în mai multe zone de pe glob.

❖ Recuperare de date

În caz de dezastru, recuperarea datelor este făcută de către furnizor, care se folosește de celelalte zone de stocare, plasate geografic strategic.

❖ **Mobilitate**

Scopul serviciilor cloud este ca acestea să poată fi accesate de oriunde, oricând și de pe orice dispozitiv, mobil sau nu.

❖ **Individualitate**

Cloud oferă soluții adaptabile oricăror cerințe pe care le poate avea o companie.

❖ **Ecologie**

Înainte infrastructurile proprii folosite de companii funcționau permanent dar prin cloud, odată cu utilizarea de resurse doar la cerere, scade și consumul de energie folosit.

2.1.3.2 Dezavantaje

Securitate și intimitate

Confidențialitatea datelor este considerată cea mai mare vulnerabilitate a soluției cloud, atât timp cât consumatorii nu se încred în fiabilitatea sistemelor IT deținute de furnizorii cloud ei vor ocoli acest tip de servicii. Vezi 2.1.4 Securitatea în Cloud pentru mai multe detalii.

Probleme tehnice

Buna funcționare a sistemelor IT cloud depinde de surse externe precum conectivitatea la Internet, probleme cu aceasta pot cauza perioade de nefuncționare. Alte vulnerabilități pot fi: pierderea datelor, piratarea conturilor sau a serviciilor, nesiguranța API-urilor, blocare sau abuz asupra serviciilor Cloud, persoane rău-intenționate din interiorul sistemului, insuficienta investigare și implicare sau probleme cu tehnologiile distribuite. [8]

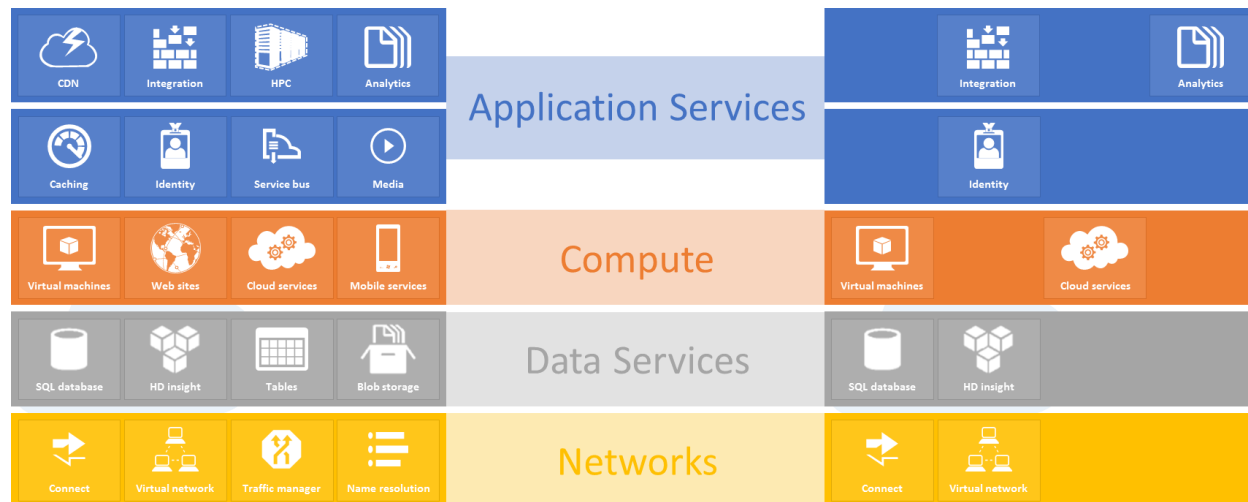
3 MICROSOFT WINDOWS AZURE

3.1 INTRODUCERE

Microsoft este unul dintre cei mai mari competitori de pe piața Cloud, oferind toate tipurile de servicii: IaaS sau mașini virtuale (Azure Virtual Machines), găzduire de site-uri și PaaS, dar și servicii SaaS prin integrarea aplicațiilor (ex: Office 365, OneDrive, Dropbox, WordPress și Amazon Kindle [9]) pentru a rula în cloud.

Soluția cloud Microsoft Azure își ia startul încă din 2006 când trei echipe cu roluri diferite încep să lucreze paralel. În doi ani se unesc complet și realizează baza platformei Windows Azure (servicii .Net, Live și SQL). După câteva luni, munca lor e recunoscută și Microsoft se remarcă pe piața cloud. [11] În următorii 5 ani noi servicii apar permanent astfel că, în prezent, Microsoft reprezintă unul dintre cei mai mari competitori, cu centre de date aflate pe tot globul, în 19 regiuni de la Melbourne, Amsterdam, Sao Paulo la Singapore și chiar și în două regiuni din China [9].

Platformele Azure oferite ca PaaS (ex: Azure Websites, Azure Cloud Services) oferă toate uneltele necesare pentru dezvoltarea și desfășurarea unei aplicații. „Windows Azure rulează în mediul virtualizat creat de Microsoft Hypervisor”, la nivel de sistem de operare sunt oferite toate tipurile de servicii, de la stocare la conectare la medii de dezvoltare de aplicații. Folosind Windows Azure SDK se pot construi aplicații în aproape orice limbaj de programare dorit, conectarea la Windows Azure făcându-se simplu, prin Internet. [8].



Figură 3.1 Serviciile Azure [10]

3.2 TIPURI DE RESURSE

În platforma sa de cloud computing, Azure oferă următoarele servicii [9, 11]:

- Servicii de **calcul** (care furnizează puterea necesară de procesare de care au nevoie aplicațiile cloud pentru a rula):
 - Cloud Services (pentru construire și desfășurare de aplicații scalabile);
 - Virtual Machines (pentru creare și plasare de mașini virtuale în cloud);
 - Websites (serviciu pentru creare de site-uri și migrarea acestora în cloud);
 - Mobile Services (pentru implementare de aplicații și stocare date pentru dispozitive mobile).
- Servicii de **date** (pentru stocare, administrare, analizare de date):
 - Microsoft Azure Storage (servicii Blob, Queue, Table și Azure Files);
 - Azure SQL Database (bază de date relațională în cadrul cloud-ului);
 - Redis Cache.
- Servicii pentru **aplicații** (unelte pentru construirea și operarea aplicațiilor):
 - Azure Active Directory;
 - Service Bus (pentru conectarea sistemelor distribuite);
 - HDInsight (pentru procesarea de “big data”, adică cantități nestructurate imense de date);
 - Azure Scheduler;
 - Azure Media Services.
- Servicii de **rețea** (oferă posibilitatea de a alege modul în care aplicațiile sunt livrate către utilizatori și centrele de date):
 - Virtual Networks (permite folosirea cloud-ului oferit de Azure ca o extensie la sistemul existent al consumatorului);
 - Azure Content Delivery Network (proiectat pentru trimite fișiere audio, video, imagini, aplicații și altele într-un mod rapid între servere apropiate ca distanță);
 - Azure Traffic Manager (permite dirijarea traficului către centrele de date Microsoft Azure în trei modalități: pentru performanța cea mai optimă, în ordine, pe rând sau folosind configurația Active/Passive).
- Servicii de **monitorizare** (pe acestea le vom elabora la punctul 3.3).

3.2.1 Azure Active Directory

Azure AD este un serviciu robust și securizat care stochează și furnizează informații despre identitatea utilizatorilor și administrare de acces, printr-un Rest API. Acest lucru permite ca o varietate mare de aplicații să poată accesa informațiile din acest serviciu, însăși serviciile Microsoft se folosesc de acesta. [11]

3.2.2 Azure Virtual Machines

Acest serviciu IaaS suportă plasarea unui server Microsoft sau unei mașini virtuale Linux într-un centru de date Microsoft Azure. Asupra clientului revin toate responsabilitățile și libertatea de configurare, mentenanță, instalare și actualizare de software. [9] Toată această configurare a mașinii este accesibilă din portalul oferit de Azure.

3.2.3 Azure Websites

Azure Websites este un serviciu cloud folosit pentru găzduirea rapidă a unei aplicații web fără nevoia de a configura sau seta mașina virtuală pe care va rula. Limbajele de programare suportate sunt .Net, Java, PHP, Node.js și Python. În plus, există deja aplicații web care pot fi folosite personalizat precum WordPress, Umbraco, Joomla! Și Drupal. Când se face o modificare asupra aplicației și se aplică comiterea ei se face actualizarea site-ului instantaneu dacă este conectat cu *Team Foundation Server* (TFS). TFS, tot un produs Microsoft și asemănător Git-ului, reprezintă o ușoară modalitate de control asupra codului sursă, individual sau în lucrul în echipă, și monitorizare prin rapoarte despre testare și rezultatele *build*-urilor efectuate (compilării codului). [9, 11]

Pentru diagnosticare, se colectează statistici despre performanță, date despre aplicație și server iar dacă apare o problemă, se poate face diagnosticarea chiar din *Microsoft Visual Studio* în timp ce aplicația rulează în cloud. [9] Visual Studio este un mediu de dezvoltare produs de Microsoft cu ajutorul căruia se poate crea aproape orice tip de aplicație în aproape orice limbaj de programare dorit. Folosind unul din portalele oferite de Azure, se pot configura multiple detalii, setări despre colectarea datelor, preferințe și rapoarte asupra aplicației.

3.2.4 Event Hub

Pe lângă faptul că platforma de streaming a datelor Azure Event Hubs este extrem de scalabilă, aceasta reprezintă și un serviciu de procesare a evenimentelor, capabilă să proceseze

milioane de evenimente pe secundă. Event Hubs poate să proceseze și să salveze informațiile asupra evenimentelor, date sau valori telemetrice rezultate din alte aplicații sau device-uri. Datele transmise către un Event Hub pot fi transformate și stocate folosind orice provider de real-time analytics sau adaptor batch/storage. Datorită abilității de a publica și recepționa date aproape în timp real la o scală mare, Event Hubs reprezintă punctul de plecare pentru Big Data. [12]

3.2.5 Azure Storage

Serviciul Storage furnizează mai multe tipuri de servicii: Blob, File Share, Table și Queue; pentru fiecare dintre acestea el asigură integritatea și mentenanța datelor, în plus și un sistem de monitorizare și alerte în cazul în care apar probleme. [9]

3.2.5.1 Blob Storage

Un „blob” reprezintă un obiect binar larg, adică fișiere comune stocate în calculatorul personal precum poze, fișiere Excel, Word, HTML, aproape orice. Prin serviciul Azure Blob accesul la aceste fișiere se poate face de oriunde din lume folosind un simplu URL (Uniform Resource Locator), o interfață REST sau una dintre librăriile Azure SDK puse la dispoziție. Mai multe blob-uri sunt puse într-un așa numit container, a cărui rol este asemenea unui folder. Deși un container nu poate conține mai multe containere, deci există un singur nivel de ierarhie printre acestea, există o modalitate de a simula un sistem de nivele folosind în numele containerelor caracterul */*. Există două tipuri de blob-uri: *block* și *page*.

Blob-urile Block sunt utilizate pentru fișiere normale cu o limită de 200 GB în mărime. Acest tip este destinat citirii de la început până la sfârșit, cum ar fi a fișierelor media. Blob-urile Block care depășesc 64 MB vin încărcate în blob-uri mai mici (*small blobs*) care apoi se consolidează într-un blob final. [9] Page blob este folosit pentru accesarea aleatorie a datelor din el deci suportă o mărime mai mare, de maxim 1 TB.

3.2.5.2 Table Storage

Tabelele furnizate de Azure folosesc modelul *NoSQL* de bază de date, permițând stocarea unor cantități imense de date semistructurate și non-relaționale. Nu sunt permise operații complexe de *join*, folosirea de chei străine cât nici executarea de proceduri stocate. Fiecare tabel are un index unic asupra căruia se pot face interogări rapid. Datele se mai pot accesa și folosind interogările LINQ. [9, 11]

Fiecare rând din tabel reprezintă o entitate care conține, pe lângă datele proprii, trei proprietăți: *partition key* (cheie de partiție), *row key* (cheia înregistrării) și un *timestamp* (marcaj de timp). Combinația dintre primele două trebuie să fie unică, împreună formează cheia primară a tabelului. Partition key permite stocarea pe noduri, toate înregistrările cu aceeași cheie de partiție sunt distribuite în același nod. Row key permite unicitatea acestor înregistrări în cadrul acelui nod. [11]

O atenție deosebită trebuie acordată modului în care se setează cheile de partiție și înregistrare pentru o cât mai bună performanță în regăsirea datelor. Cea de-a treia cheie, marcajul de timp este setat implicit de Azure și reprezintă momentul de timp în care s-a făcut ultima modificare asupra înregistrării. [9]

3.2.5.3 Queues

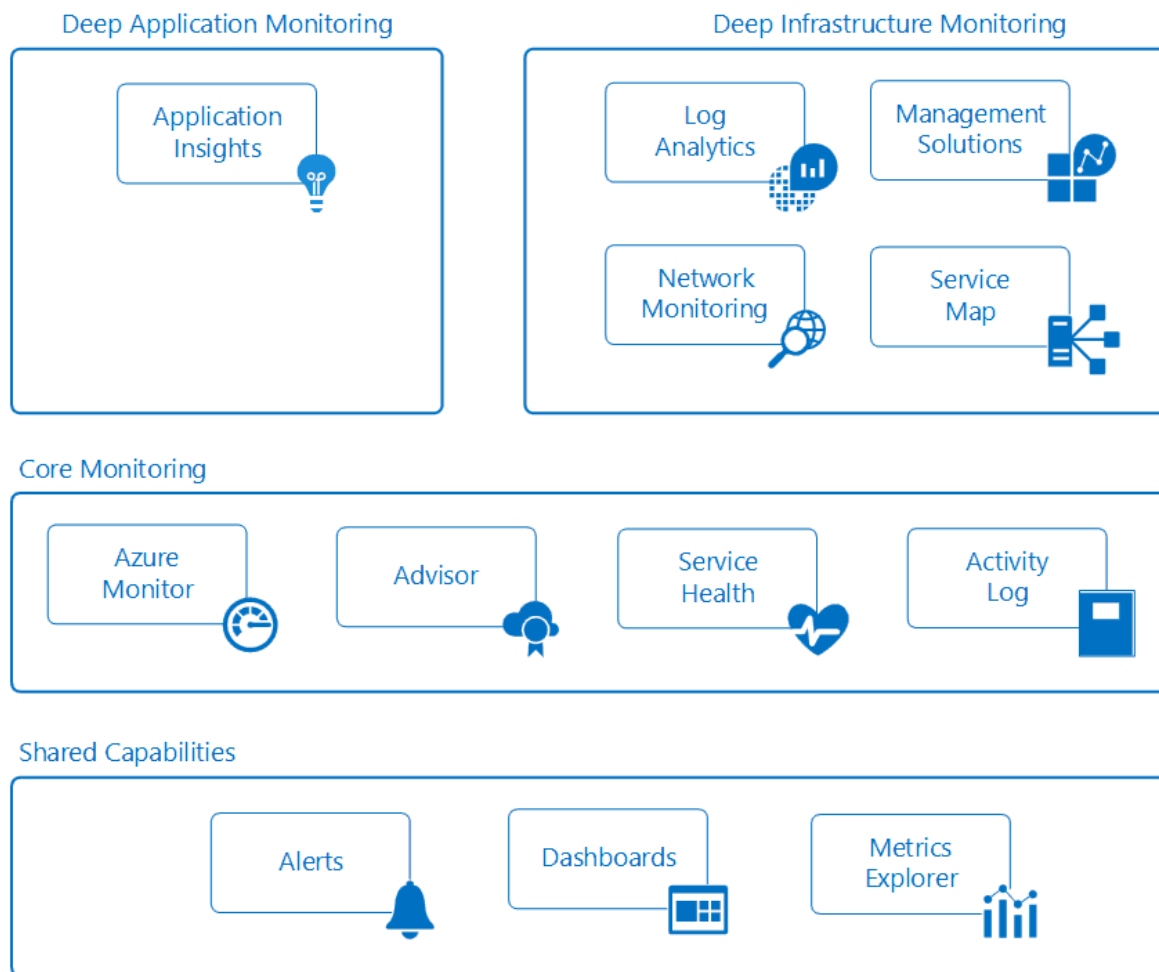
Acest serviciu este folosit pentru a stoca și a extrage liste de mesaje procesate asincron, după modelul FIFO (first in, first out). Mesajele nu pot depăși mărimea de 64 KB, astfel, o coadă (queue) poate ajunge să conțină milioane de mesaje. [9]

3.3 SERVICIILE AZURE DE MONITORIZARE

Monitorizarea unei aplicații constă în colectarea și analizarea datelor cu scopul determinării performanțelor, buna funcționare („sănătatea”) aplicației și a resurselor de care depinde. Putem spune că o monitorizare eficientă constă în stabilirea unei strategii care are capacitatea de extragere a operațiilor detaliate asupra componentelor aplicației. De asemenea, în cazul apariției unor probleme critice, notificarea persoanelor responsabile pentru punerea componentelor înapoi în funcțiune sau soluționarea lor.

Azure dispune de multiple servicii care au roluri și funcționalități specifice fiecăruia. Împreună aceste servicii oferă o soluție vastă de colectare, analizare și acționare asupra rezultatelor obținute din aplicația proprie și a resurselor compuse în aceasta. Este posibilă și monitorizarea infrastructurilor on-premise, înțelegerea tuturor soluțiilor pe care Azure le oferă în scopul monitorizării este de preferat înaintea alegerii celei mai potrivită și completă strategie.

Următoarea diagramă oferă o prezentare generală și conceptuală asupra componentelor care împreună oferă soluția Azure de monitorizare.



Figură 3.2 Servicii de monitorizare în Azure [13]

După cum putem vedea, în partea de jos avem secțiunea care cuprinde funcționalități generice (Shared capabilities), acestea fiind utilizabile și în serviciile conținute în secțiunile de mai sus: Deep Application Monitoring, Deep Infrastructure Monitoring și Core Monitoring.

3.3.1 Serviciile Shared Capabilities

3.3.1.1 Alerte

Se pot defini alerte care te notifică în cazul apariției unor condiții critice și au potențial de a lua și măsuri corective. Acestea se definesc prin stabilirea unor reguli care pot folosi date din mai multe surse, inclusiv metrice și fișiere de loguri.

3.3.1.2 *Tablouri de bord*

De asemenea se pot crea *tablouri de bord* particulare în portalul Azure care pot fi distribuite și altor utilizatori. De exemplu un graf de metrice, tabel de loguri asupra activității, o statistica din Application Insights sau output al unui log de căutare din Log Analytics.

Informația generată de serviciul Log Analytics se poate exporta în Power BI, de unde se pot construi moduri de vizualizare mai avansate. De asemenea se pot exporta pentru a fi vizibile și în afara organizației

3.3.1.3 *Metrics Explorer*

Metricile sunt valori numerice generate de o resursă azure cu scopul de a ajuta la înțelegerea operațiilor și performanței a unei resurse. Metrics Explorer este un program prin care se pot trimite metrice la Log Analytics pentru analizare împreună cu informații provenite din alte surse.

3.3.2 *Core Monitoring*

Acest set de componente oferă informațiile de monitorizare de bază a resurselor Azure. Aceste servicii necesită configurări minime și colectează măsurători de bază pe care le folosesc serviciile de monitorizare premium.

3.3.2.1 *Azure Monitor*

Azure Monitor permite monitorizarea de bază asupra serviciilor Azure prin colectarea metricilor, logurilor de activitate și de diagnostic. De exemplu, logurile de activități (provenite din Activity Log) rețin timpul creării, modificării sau ștergerii resurselor.

Metricile pun la dispoziție statistici de performanță pentru diferite tipuri de resurse, până și despre sistemele de operare dintr-o mașină virtuală. Acestea pot fi vizualizate din portal și se pot crea alerte bazate pe acestea. Pot fi folosite cu încredere pentru a genera notificări în cazuri critice deoarece, aceste metrice pot fi obținute odată la cinci minute, chiar și la un minut.

3.3.2.2 *Azure Advisor*

Face aceleași colectări ca și Azure Monitor, pe lângă asta oferă recomandări personalizate bazate pe practicile utilizate des și recomandate. Urmând aceste recomandări se obțin îmbunătățiri asupra performanței și securității resurselor ce compun aplicația.

3.3.2.3 *Service Health*

Sănătatea aplicației se bazează pe servicii Azure de care depinde. Cu acestea spuse, Azure Service Health identifică probleme ce pot apărea cu acestea și care pot afecta buna funcționare a aplicației. Este posibilă și programarea unui plan de întreținere a acestora.

3.3.2.4 *Activity Log*

Activity Log furnizează date despre operațiile efectuate asupra unei resurse Azure. Aceste informații pot fi:

- Schimbări în configurația acestora
- Incidente Service health
- Recomandări pentru utilizarea acestora
- Informații legate de scalarea automată a operațiilor

Se pot vedea logurile unei resurse particulare în portal pe pagina respectivă resursei, se poate folosi și Activity Log Explorer pentru vizionarea logurilor provenite din mai multe resurse.

3.3.3 *Serviciile Deep Monitoring*

Următoarele servicii Azure au capacități vaste de colectare și analizare a informațiilor de monitorizare la un nivel mai profund. Aceste servicii construite pe acelea de la Core Monitoring oferă analize elocvente pentru a beneficia de viziuni perspicace asupra aplicației sau infrastructurii și a prezenta datele în contextul unor scenarii vizate pe anumite audiențe.

3.3.3.1 *Application Insights*

Acest serviciu este intenționat spre monitorizarea aplicațiilor din cloud sau on-premise punând la dispoziție date despre performanță și folosință, putând face alegeri informate asupra mentenanței și îmbunătățiri aduse acesteia. Prin instrumentarea aplicației cu acest serviciu se pot obține perspective profunde și de asemenea implementări de scenarii DevOps, identificarea și

diagnosticarea erorilor sunt obținute imediat înaintea ca acestea să fie raportate de utilizator și astfel prevenind situații neplăcute.

Sunt puse la dispoziție unele instrumente extinse pentru interacțiunea cu datele pe care le colectează, stocate într-un spațiu comun. Pot fi integrate cu funcționalitățile generice prezentate mai înainte precum alerte, tablouri de bord și analiză profundă cu limbajul de interogare oferit de Log Analytics.

Sistemul de Smart Detection oferă alerte despre potențiale probleme de performanță a aplicației web. Acest sistem analizează proactiv datele telemetrice transmise de către aplicație către Application Insights. În cazul unor creșteri rapide a numărului de erori, a unor tipare anormale în urma acțiunii clienților sau în cazul variațiilor mari a indicilor de performanță, utilizatorul primește un mesaj de alertă. [14]

Această funcționalitate nu necesită nici o configurare, aceasta fiind activă dacă aplicația trimite un volum destul de mare de date telemetrice,

3.3.4 Serviciile Deep Infrastructure Monitoring

3.3.4.1 Log Analytics

Poate serviciul care joacă rolul cel mai central în monitorizarea resurselor prin colectarea datelor asupra unei varietăți mari de resurse, inclusiv non-Microsoft, într-un singur spațiu. Acolo se pot interoga și analiza datele printr-un limbaj de interogare vast.

Application Insights și Azure Security Center își stochează datele în spațiul de stocare al serviciului Log Analytics și folosesc capabilitățile lui de analiză. Date sunt colectate de asemenea și din Azure Monitor și agenți instalați pe mașinile virtuale în cloud sau on-premise. Acestea prezentate putem concluda că împreună oferă o viziune completă asupra mediului conturat în jurul aplicației.

3.3.4.2 Management Solutions

Management solutions sunt disponibile din partea Microsoft și partenerii lui pentru a oferi monitorizare pentru Azure și servicii third-party. Exemple de soluții ar fi monitorizarea containerelor (Container Monitoring) și Azure SQL Analytics care colectează și reține date asupra performanței bazelor de date SQL găzduite în Azure cloud. Toate exemplele se pot vedea în portal în secțiunea Monitor.

3.3.4.3 Network Monitoring

Instrumente disponibile pentru a superviza rețeaua din cloud sau on-premise sunt puse la dispoziție precum

1. Network Watcher – livrează monitorizare bazată pe scenarii și diagnostic pentru diverse scenarii rețelistice în Azure. Își stochează datele în Azure metrics și diagnostice pentru analize adiționale. Este folosit cu soluțiile ce urmează pentru a monitoriza diverse aspecte asupra rețelei utilizatorului.
2. Network Performance Monitor (NPM) este o soluție de monitorizare a rețelelor, bazată pe cloud, asupra conectivității dintre cloud-uri publice, centre de date și infrastructuri on-premise.
3. ExpressRoute Monitor este o capabilitate în NPM care monitorizează conectivitatea end-to-end și performanța asupra circuitelor Azure ExpressRoute.
4. DNS Analytics este o soluție care livrează date legate de securitate, performanță și operațiile efectuate în serverele DNS.
5. Service Endpoint Monitor - testează accesibilitatea aplicațiilor și pândește locurile unde s-ar putea efectua blocaje.

3.3.4.4 Service Map

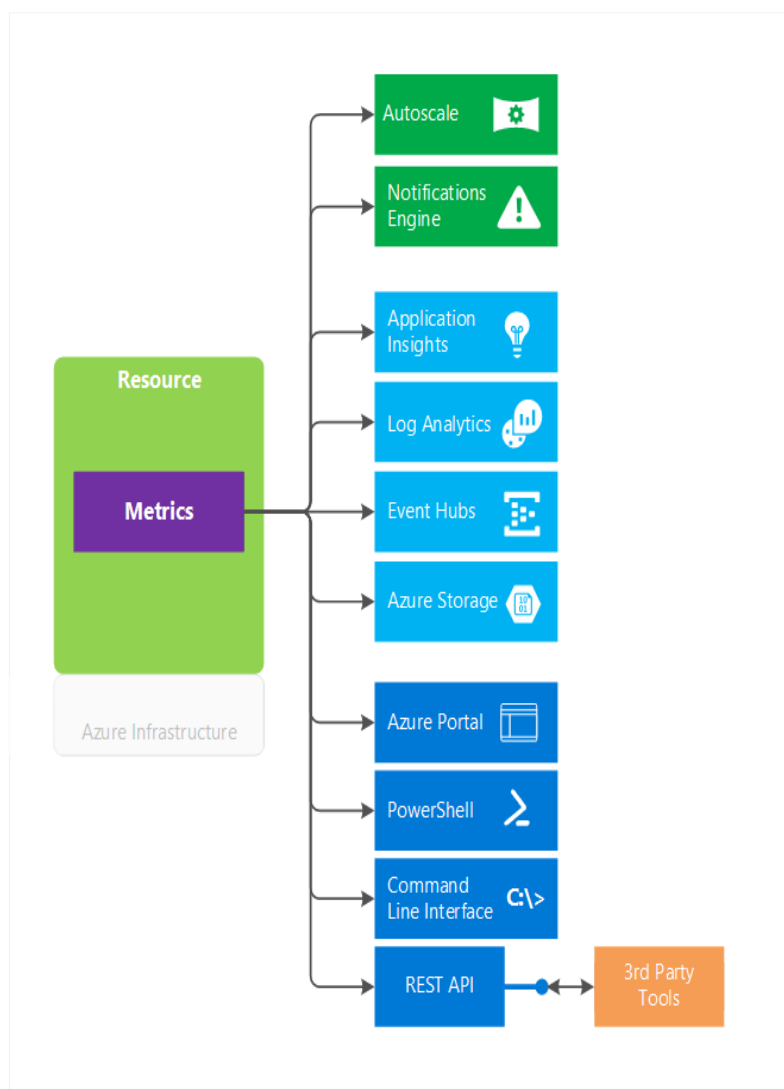
Service map este similar ca funcționalitate cu Application Map din cadrul serviciului Application Insights prin faptul că se concentrează asupra componentelor care compun infrastructura aplicației. Funcționează deci cu tipul de modelul de cloud IaaS prin analizarea mașinilor virtuale și proceselor, dependențelor cu alte calculatoare sau procese externe. Aceste informații le exportă în Log Analytics, unde se poate vedea pentru fiecare calculator, date despre interacțiunea acestuia cu „lumea” exterioară.

4 METRICI

4.1 PREZENTARE GENERALĂ

Azure Monitor ne permite să interpretăm date telemetrice pentru a putea urmări performanța și integritatea sistemelor în Azure. Cel mai important tip de date telemetrice din Azure sunt metricele, denumite și indici de performanță (performance counters) prezente în majoritatea resurselor Azure. Azure Monitor ne oferă mai multe posibilități de a configura și citi metrici pentru monitorizare și depanare a sistemelor.

Metriicii prezintă următoarele caracteristici:



- Toți metriicii au o periodicitate standard de un minut (aceasta poate fi determinata de catre utilizator). O dată pe minut, utilizatorul primește valoarea metricului resursei, astfel oferind informații în timp real despre starea și integritatea acesteia.
- Valorile metrice sunt disponibile fără necesitatea de a configura sistemele de diagnoză complexe.
- Fiecare metric este disponibil timp de o perioadă de 93 de zile, oferind posibilitatea de a urmări date recente, dar și de a urmări trendurile lunare ale integrității și performanței sistemului. Unele metrice pot avea perechi de attribute nume-valoare denumite dimensiuni. Acestea permit utilizatorului urmărirea în detaliu a metricului respectiv.

Figură 4.1 Metrici și servicii[15]

4.2 METRICI DE BAZĂ

Pentru urmărirea metricilor se pot defini următoarele taskuri:

- Se pot configura reguli pentru a trimite alerte sau pentru a executa anumite acțiuni în cazul depășirii pragului limită definit. Aceste acțiuni sunt controlate prin grupuri de acțiuni. Exemple pentru astfel de acțiuni ar fi notificări trimise prin email, telefonic, sms, apeluri către un webhook, inițializarea unui runbook și multe altele. O acțiune automatizată specială ar fi Autoscale. Aceasta ne permite să scalăm resursa, măbind sau diminuând valorile ei, pentru a reduce costurile în perioadele de utilizare sub sarcină. O astfel de regulă se poate configura pentru orice metric care depășește un prag superior și inferior definit de utilizator.
- Toți metricii pot fi transferați către Application Insights sau Log Analytics astfel încât să se poată efectua căutări și crea alerte mai specifice pentru valorile metricilor resurselor.
- O altă opțiune este transmiterea metricilor către un Event Hub, astfel permițând redirecționarea lor către Azure Stream Analytics sau către alte aplicații pentru o analiză în timp real a valorilor. Transmiterea de date către Event Hub se configurează folosind configurațiile de diagnosticare.
- Se oferă posibilitatea de a arhiva datele despre performanța sau integritatea resurselor pentru analiză sau creare de rapoarte. Valorile metricilor pot fi direcționate către stocare în Azure Blob în momentul configurării setărilor de diagnosticare pentru fiecare resursă în parte.
- Portalul Azure este folosit pentru a accesa toate valorile metricilor în momentul selecției unei resurse și se dorește afișarea valorilor sub forma unei diagrame. Performanța unei astfel de resurse, precum o mașină virtuală, un site sau o aplicație, poate fi urmărită mai ușor prin adăugarea diagramei aferente în spațiul de lucru.
- Se pot extrage rapoarte sau date analitice complexe despre performanța resurselor sau staticile de utilizare a acestora.
- Acești metriCI pot fi interogați prin comenzi PowerShell sau folosind REST API.
- Azure Monitor REST API-uri pot fi folosite pentru a importa valorile metricilor.

4.3 METRICI MULTI-DIMENSIONALI

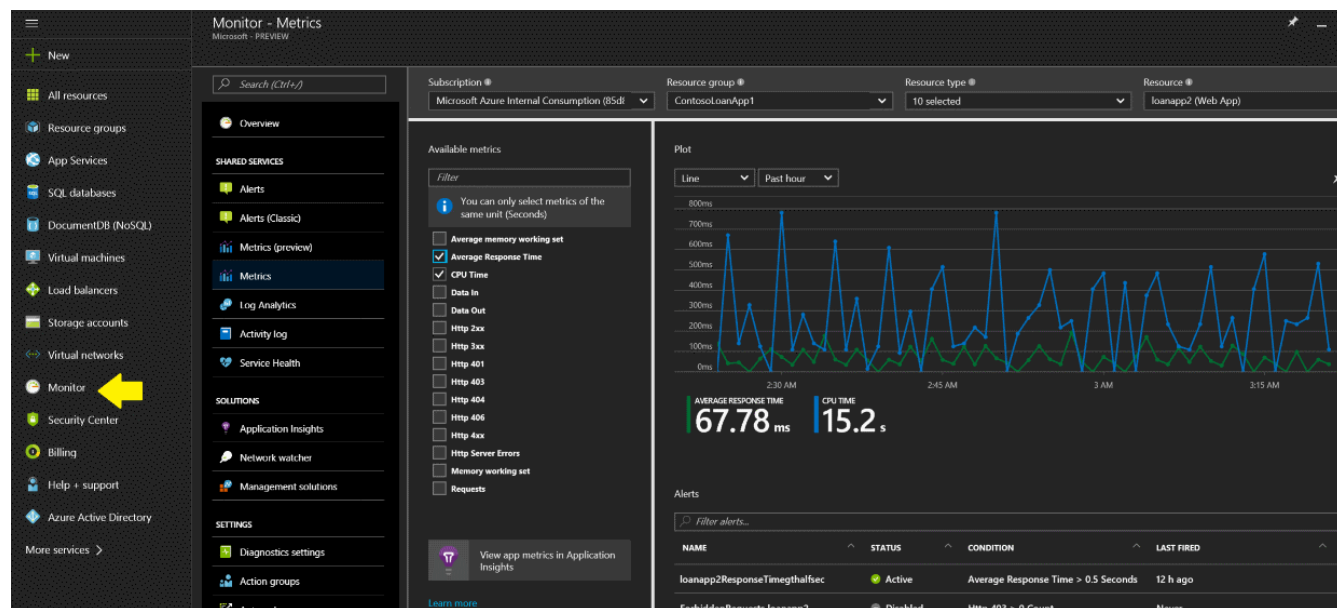
Majoritatea resurselor din Azure expun acum metrici multidimensionale. Aceste metrici urmăresc mai multe seturi de valori pentru una sau mai multe dimensiuni. De exemplu, un metric precum spațiul liber de stocare ("Available disk space") poate avea dimensiuni precum "Drive" cu valorile "C:", "D:" care oferă posibilitatea de a vizualiza spațiul liber al tuturor partițiilor sau a tuturor mediilor de stocare, sau a partițiilor individuale și a fiecărui mediu de stocare. [16]

4.4 INTEROGAREA METRICILOR

Vom alege ca și caz de studiu mașinile virtuale. Indiferent de sistemul de operare, Linux sau Windows, se dorește monitorizarea metricilor de bază pentru a asigura funcționarea serviciilor și a serverelor. Cele mai relevante metrici pentru acest tip de resursă sunt CPU, disk I/O, utilizarea memoriei și traficul. Pentru o mașină virtuală, există 5 alternative de obținere a metricilor, următoarele 2 destinate utilizatorilor obișnuiți:

4.4.1 Azure Portal

Prin intermediul portalului Azure se pot selecta simplu metricile și se pot crea alerte. Acest portal poate fi folosit cu ușurință de către utilizatorul de rând.

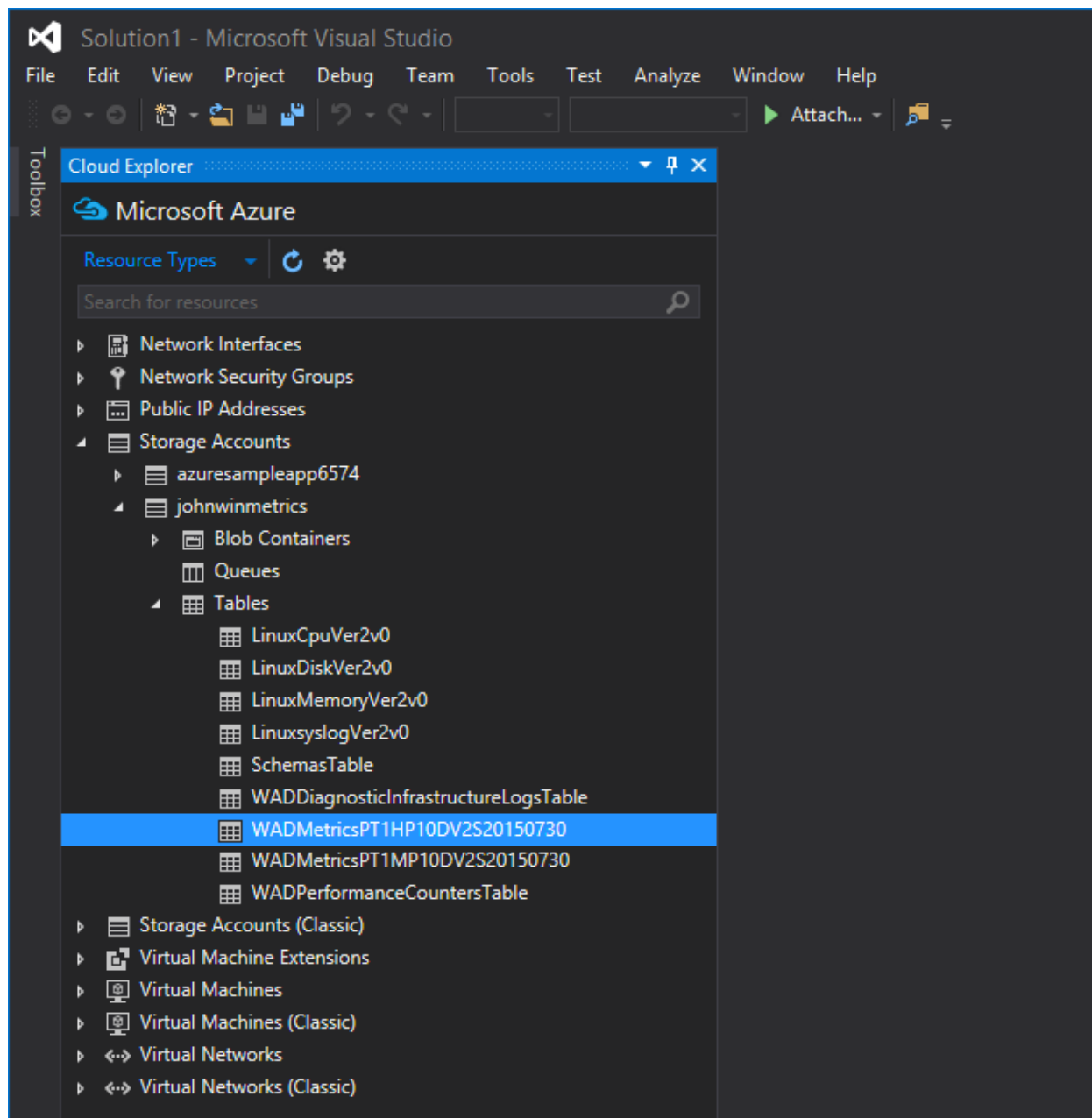


Figură 4.2 Azure portal monitor

4.4.2 Azure storage

Această soluție implică mai mulți pași. Se începe cu activarea extensiei de Azure Diagnostics în proprietățile mașinii virtuale pentru care se dorește obținerea de loguri în format neprocesat.

Aceste loguri sunt stocate într-un storage account, deci este nevoie de crearea acestuia. Apoi, în Visual Studio, în fereastra Cloud Explorer vom vedea tabelele cu informațiile despre metricile acelei mașini virtuale. care mai apoi se pot exporta.



Figură 4.3 Cloud explorer Azure tables

4.4.3 Azure CLI & Powershell

Un exemplu de request azure cli care ia metricile de tip Percentage CPU din ultima oră:

```
az monitor metrics list --resource {ResourceName} --metric "Percentage CPU"
```

Un alt exemplu de script powershell care ia valoarea medie CPU la interval de 1 minut pentru ultimele 40 de minute.

```
$endTime = Get-Date
$startTime = $endTime.AddMinutes(-40)
$timeGrain = '00:01:00'
$resourceId =
'/subscriptions/SUBSCRIPTION_guid/resourceGroups/myRG/providers/Microsoft.Compute/virtualMachines/myVM'
$metricName = '\Processor(_Total)\% Processor Time'

(Get-AzureRmMetric -ResourceId $resourceId `
-TimeGrain $timeGrain -StartTime $startTime `
-EndTime $endTime `
-MetricNames $metricName).MetricDefinitions
```

4.4.4 REST API

Metricile Azure sunt accesibile prin API-urile Azure Monitor. Sunt puse la dispoziție două API-uri pentru accesarea acestora.

1. Azure Monitor Metric Definitions REST API, care obține lista de metrici basic sau multi-dimensională disponibili pentru o resursă, inclusiv detalii despre dimensiunile existente.
2. Azure Monitor Metrics REST API, pentru a segmenta, filtra și accesa actualele valorile ale metricilor.

Formatul de bază pentru request-ul de metrici:

```
GET
https://management.azure.com/{resourceUri}/providers/microsoft.insights/metrics?timespan=
{timespan}&interval={interval}&metricnames={metricnames}&aggregation={aggregation}&
top={top}&orderby={orderby}&$filter={$filter}&resultType={resultType}&api-
version=2018-01-01&metricnamespace={metricnamespace}
```

5 DEZVOLTAREA APLICATIVĂ

5.1 PREZENTARE

Aplicația prezentată în cadrul acestei lucrări reprezintă un sistem de colectare și procesare a metricilor care poate fi modificat oricând pentru a împlini cerințe noi. Aplicația propune o idee de implementare a unui sistem de monitorizare particularizat pe nevoile utilizatorului, cu mențiunea că se urmărește totuși ca serviciile monitorizate să fie de tipul resurselor din cloud pe care se bazează aplicația acestuia.

Aplicația pune la dispoziție interogarea de metrice pentru patru resurse importante și general cunoscut din Azure. Storage Accounts, Websites, Virtual Machines și Event Hubs sunt doar câteva din cele cunoscute dar indeajuns pentru scopul demonstrativ al acestei aplicații.

Pentru interogarea datelor abordarea inițială a fost folosirea unor librării Azure, accesibile ca pachete nuget. Există un pachet din 2013 dar este out-dated, așa că s-a încercat implementarea folosind Monitor Library pentru mașini virtuale și Insights Library pentru mașinile virtuale clasice și aplicații web. Aceste pachete sunt în faza preview și se aduc modificări actuale destul de rar. Folosirea acestor pachete a fost anevoioasă din cauza dependențelor la versiuni vechi de dll-uri precum Newtonsoft.JSON, dar autentificarea necesita versiune mai nouă. Astfel spus, în loc ca implementarea să fie mai rapidă prin folosirea unor librării cu clase clar predefinite, lucru care nu s-a putut, s-a recurs la varianta simplă de creare a unor request-uri HTTP de get la API-urile de monitorizare dispuse de Azure.

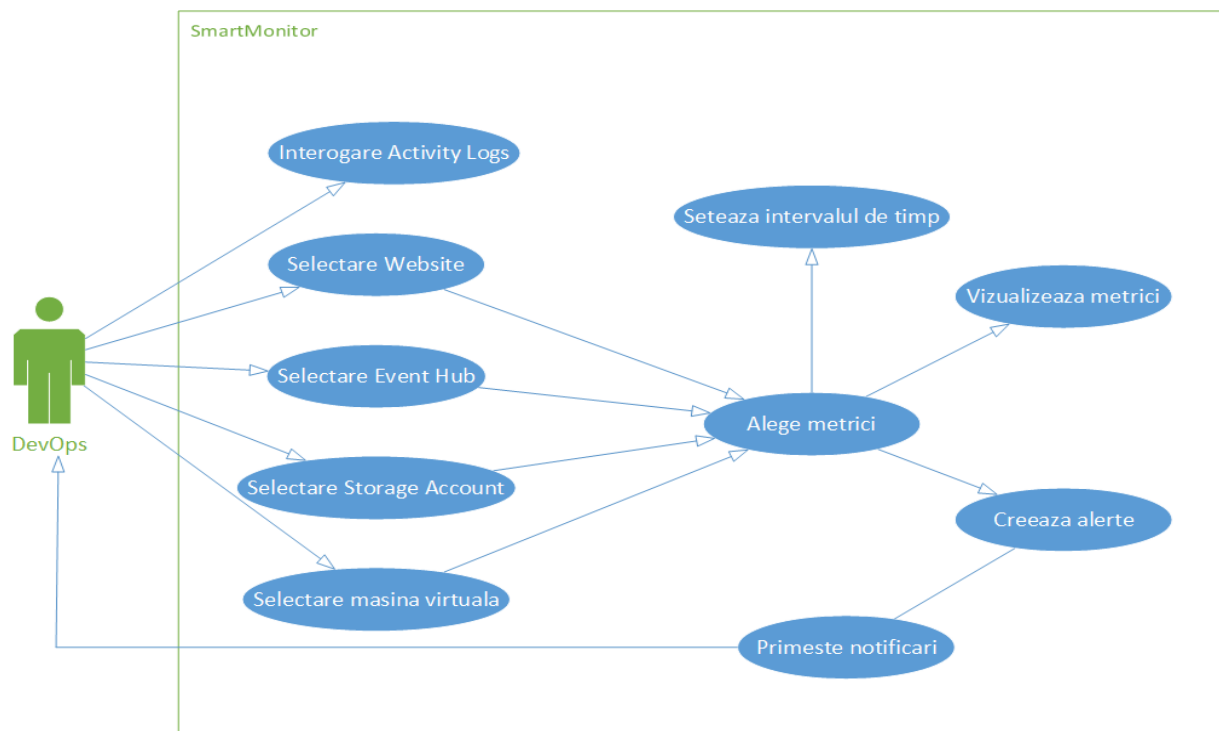
Rezultatele provenite din aceste call-uri reprezintă JSON-uri care au fost parsate și create modele după pentru a fi parsate cu ușurință în GUI.

5.2 TEHNOLOGII

Pentru proiectarea acesteia au fost create diagrame draw.io și Microsoft Visio. Pentru crearea resurselor cloud care să fie monitorizate s-au folosit portalele oferite de Azure dar și scripturi Powershell. Pentru implementarea aplicației, limbajul de programare C#, în mediul de dezvoltare Visual Studio, integrare cu Git Hub. Tehnologia utilizată pentru realizarea interfeței grafice cu utilizatorul a fost Windows Forms alături de pachetul nuget MetroModernUI, un framework open source care aduce îmbunătățiri estetice, împreună cu LiveCharts pentru statistici.

5.3 PROIECTARE

5.3.1 Cazuri de utilizare



Figură 5.1 Diagrama de cazuri de utilizare

Utilizatorului îi este pus la dispoziție o aplicație grafică foarte asemănătoare celor existente în cadrul Microsoft. El nu mai este nevoie să se logheze, deoarece în spate se face inițierea conexiunii bazată pe credențialele deja setate. Dacă aceasta s-a efectuat cu succes, atunci există patru importante cazuri de utilizare.

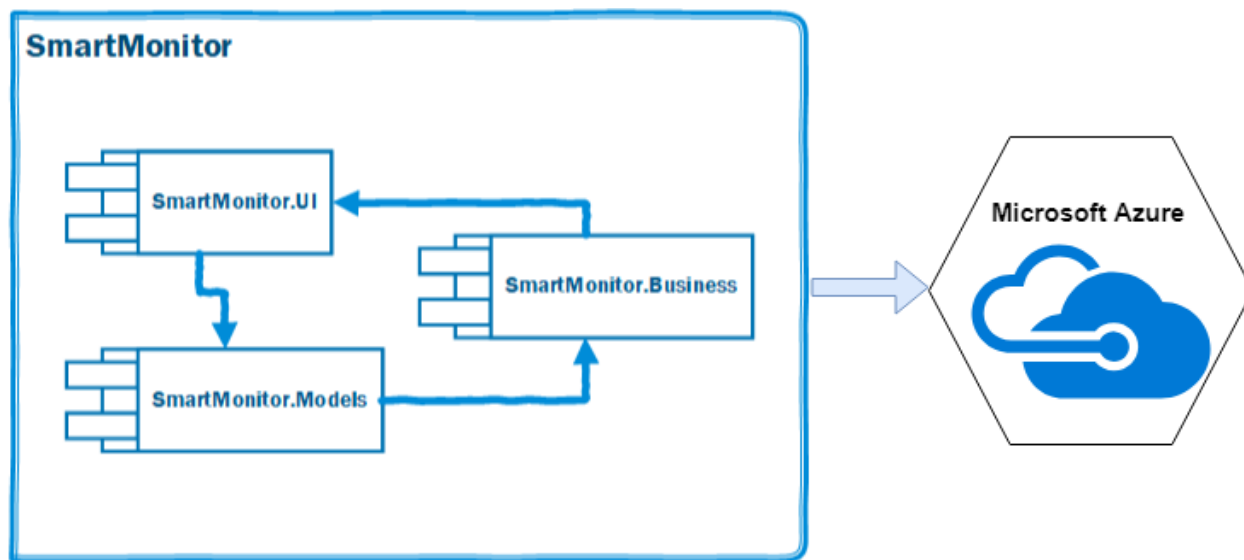
Pentru fiecare tip de resursă implementat, se pot efectua următoarele operații:

❖ **Selectează tipul de resursă dorit a fi monitorizat:**

- **Selectează resursa dorită** (utilizatorul aplicației are opțiunea de a vizualiza toate resursele de acel tip (de ex: website-urile) din subscripție);
- **Alege metrice** (se va afișa toate definițiile de metrice disponibile care există pentru acest tip de resursă);
- **Selectare metrice** (utilizatorul are la dispoziție un set de statistici vizuale pentru urmărirea metricilor);

- **Setare interval de timp** (pentru a seta cel dorit și a chestiona metricile din acea perioadă);
- **Creează alerte** (pentru a primi notificări în urma nerespectării regulii alertei setate)

5.3.2 Componentele aplicației



Figură 5.2 Diagrama de componente

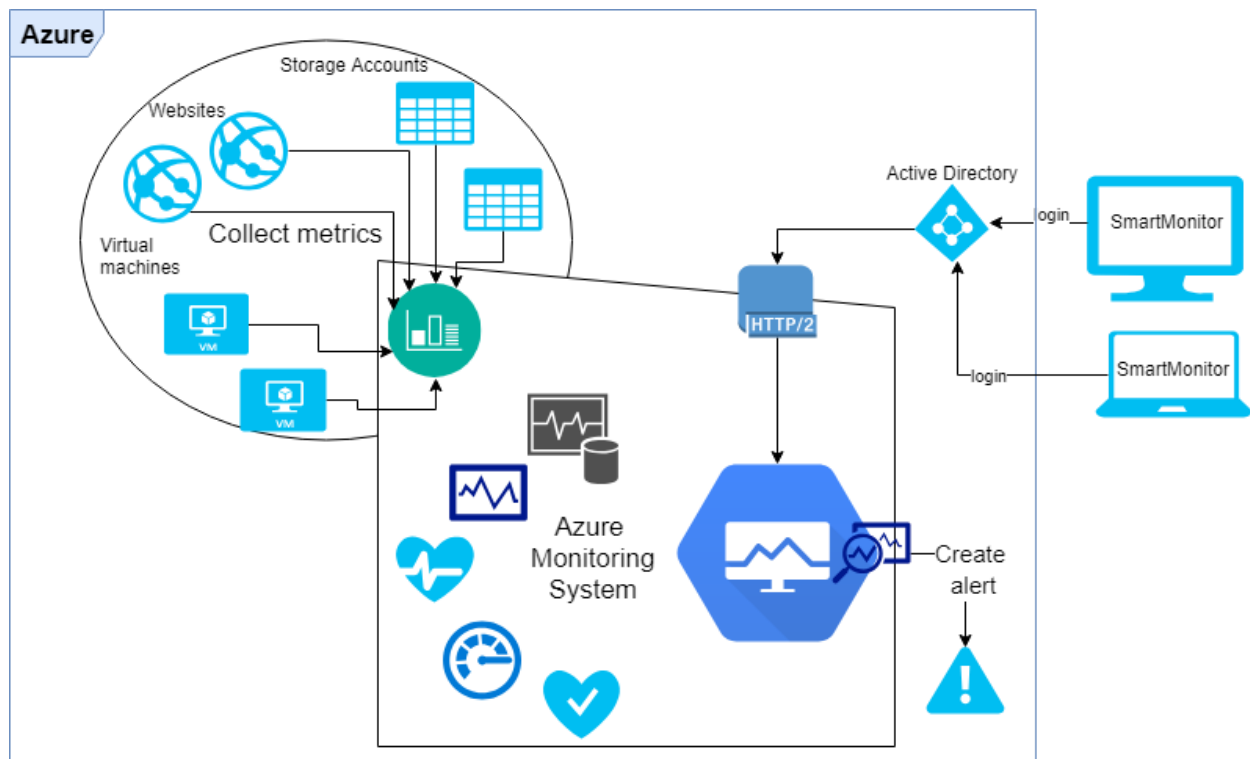
Aplicația este împărțită pe 3 componente. Este similară cu modelul MVC (Model-View-Controller) în sensul că există o componentă a entităților, una a implementării grafice și cea a serviciilor.

În componenta de entități, SmartMonitor.Models sunt definite în clase obiectele ce sunt returnate de la sistemul de monitorizare Azure. Astfel există un set de clase pentru definițiile de metrici, pentru metrici, pentru alerte ș.a.

Componenta SmartMonitor.Business conține serviciile utilizate pentru a accesa serviciile de monitorizare care aparțin de Azure. Acesta conține toată logica de interogare și de trimiterea datelor specifice pentru a fi vizualizate în componenta UI.

SmartMonitor.UI este un proiect de tip WinForm, astfel dezvoltarea s-a făcut pe tehnologia Windows Forms de la Microsoft. Acesta populează controalele cu date obținute din componenta de servicii și conține logica de parsare a metricilor pe graficele implementate.

5.3.3 Diagrama de arhitectură



Figură 5.3 Diagrama de arhitectură

5.4 COLECTAREA METRICILOR

Pentru colectarea metricilor s-au folosit API-urile puse la dispoziție de Azure Monitor, prin call-uri HTTP REST pentru obținerea întâi a definițiilor de metrice și apoi pentru valorile efective ale acestora.

Pentru crearea de alerte s-a folosit tot HTTP calls, la fel și pentru interogarea alertelor deja existente.

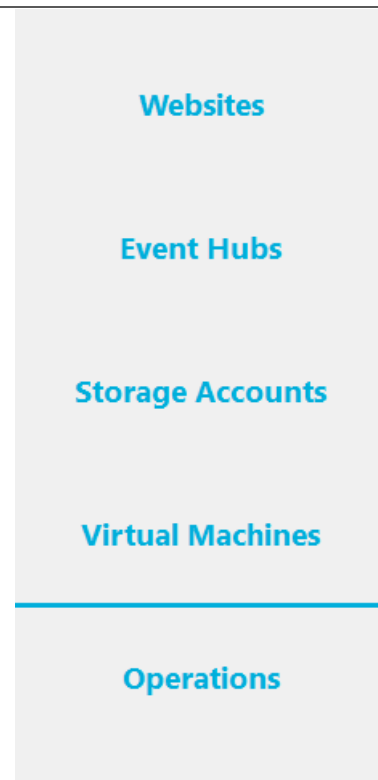
Rezultatele request-urilor HTTP au fost parsate în entități construite după modelul JSON obținut și re folosirea lor între tipuri de resurse diferite dar cu aceeași structură de date obținută ca rezultat.

6 MANUAL DE UTILIZARE

Meniul principal este unul foarte simplu, compus din tab-uri pentru fiecare set de resurse principale pentru care s-a implementat monitorizare de resurse.

Avem:

1. Aplicații web
2. EventHubs
3. Storage Accounts
4. Mașini virtuale

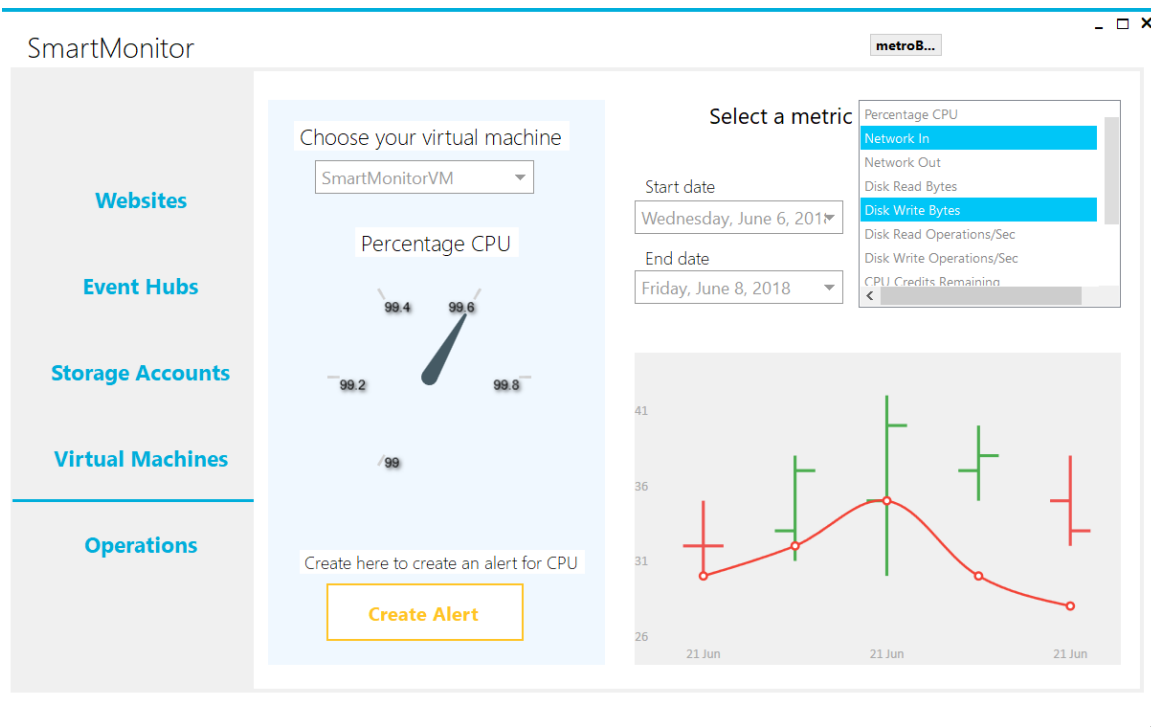


Figură 5.4 Meniul principal

Pentru fiecare tip de resursă în parte s-a construit o strategie de afișare și vizualizare a metricilor, astfel că pentru mașini virtuale va fi cel mai important metrica ce măsoară procentul CPU dar pentru aplicații web va fi răspunsul de timp al acesteia.

Pentru fiecare serviciu în parte există posibilitatea de a crea alerte, raportate la metricile specificei resursei de care face parte. Mai jos se găsesc câteva capturi de ecran care surprind funcționalitățile de filtrare a metricilor și dispunerea acestora în grafice vizuale cât și filtrarea după intervalul de timp în care se dorește investigarea acestora, în cautare de progrese sau involuții de-a lungul lunilor.

Mașini virtuale:



Figură 5.5 Tabul masini virtuale

Aplicații Web



Figură 5.4 Tabul Websites

7 CONCLUZIE

Deși informația care se învâрте în jurul creării și colectării programatice de metrice ale unei resurse este fragmentată, documentația Azure este un ghid satisfăcător în cererea și procesarea metricilor.

Modurile prin care metricele pot fi vizualizate sunt nenumărate, având valorile metricilor se pot crea cu acestea diverse grafice de vizualizare și rapoarte de statistică. Datorită faptului că metricele pot fi interogate și cu ajutorul unui filtru, cum ar fi intervalul de timp (timegrain), se pot obține rapoarte țintite pe ce dorește clientul aplicației să vadă și poate să îmbunătățească pe viitor.

O aplicație de genul acesta poate avea aplicabilitate în cadrul oricărui sistem în care performanța joacă un rol important sau în care sunt varietăți mari în numărul de request-uri pe o perioadă de timp. Un sistem financiar care este folosit foarte frecvent în anumite zile sau perioade mai lungi de timp din an ar beneficia în mare măsură de un sistem de monitorizare pus la punct, care să monitorizeze website-ul, baza de date dacă e cazul și să-i sugereze clientului să scaleze aceste resurse pentru reducerea costurilor și creșterea eficienței.

Toate aceste variațiuni în folosirea resurselor pot fi ușor găsite cu ajutor serviciilor de monitorizare corespunzătoare, și după cum am văzut, Windows Azure are un sistem vast din aceste servicii.

Pe viitor, aplicația se poate extinde înspre a monitoriza și alte tipuri de servicii precum Azure SQL database și de asemenea realiza interogări mai detaliate și mai specifice cu ajutorul filtrelor.

Amintim că aplicația prezentată este doar o propunere de implementare a unui sistem particularizat de monitorizare pentru o aplicație oarecare ce necesită a fi monitorizată și a resurselor de care depinde aceasta.

8 BIBLIOGRAFIE

- [1] Erl, Thomas, Ricardo Puttini, and Zaigham Mahmood. *Cloud computing : concepts, technology, & architecture*. Upper Saddle River, NJ: Prentice Hall, 2013.
- [2] Timothy Grance, Peter Mell. *The NIST Definition Of Cloud Computing*. 2011.
<http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf>.
- [3] Azeemi, Imran Khan, Mike Lewis, and Theo Tryfonas. *Migrating To The Cloud: Lessons And Limitations Of 'Traditional' IS Success Models*. Procedia Computer Science. 2013
- [4] Buyya, Rajkumar, James Broberg, and Andrzej Gościński. *Cloud computing principles and paradigms*. Hoboken, N.J: Wiley, 2011.
- [5] Secovia. *Overview of Cloud Computing*. 2014
<http://www.secovia.eu/news/secovia-overview-of-cloud-computing>
- [6] Mani, Sindhu, *Empirical Performance Analysis of High Performance Computing Benchmarks Across Variations in Cloud Computing* (2012). UNF Theses and Dissertations. Paper 418.
- [7] Jamsa, Kris. *Cloud computing : SaaS, PaaS, IaaS, virtualization, business models, mobile, security and more*. Burlington, MA: Jones & Bartlett Learning, 2013.
- [8] Asociația Națională pentru Securitatea Sistemelor Informatice. *Securitatea în Cloud*. 2013
http://www.cert-ro.eu/files/doc/775_20131030091057011764400_X.pdf
- [9] Michael Collier, Robin Shahan. *Microsoft Azure Essentials - Fundamentals of Azure*. Microsoft Press. 2015
- [10] How to buy Windows Azure
<https://imageframe.co.uk/how-to-buy-windows-azure/>
- [11] Mitch Tulloch. *Introducing Windows Azure for IT Professionals*. Microsoft Press. 2013
- [12] What is Event Hubs?
<https://docs.microsoft.com/en-us/azure/event-hubs/event-hubs-what-is-event-hubs>
- [13] Monitoring Azure applications and resources
<https://docs.microsoft.com/en-us/azure/monitoring-and-diagnostics/monitoring-overview>
- [14] Smart Detection in Application Insights

Bibliografie

<https://docs.microsoft.com/en-us/azure/application-insights/app-insights-proactive-diagnostics>

[15] Overview of metrics in Microsoft Azure

<https://docs.microsoft.com/en-us/azure/monitoring-and-diagnostics/monitoring-overview-metrics>

[16] Azure Monitor Metrics Explorer

<https://docs.microsoft.com/en-us/azure/monitoring-and-diagnostics/monitoring-metric-charts>