საქართველოს მეცნიერებათა ეროვნული აკადემიის მოამბე, ტ. 15, №3, 2021
BULLETIN OF THE GEORGIAN NATIONAL ACADEMY OF SCIENCES, vol. 15, no. 3, 2021

Informatics

Collection and Analysis of Log Data with Cloud Services

Otar Shonia[*], Nino Topuria[*], Konstantine Kulijanovi[**]

[*]*Georgian Technical University, Tbilisi, Georgia*
[**]*Georgian American University, Tbilisi, Georgia*

(Presented by Academy Member Gocha Chogovadze)

To achieve observability in today's complex computing environments running distributed applications that rely on cloud and local services, it is necessary to collect operational data from every layer and every component of the distributed system. It is very important to perform deep insights on this data and consolidate it into a single pane of glass with different perspectives to support the multitude of stakeholders of the organization. The article proposes Microsoft cloud services, such as Azure Monitor and Power BI and Amazon Web Services, such as Amazon CloudWatch and Kibana, for monitoring log data. Based on these services we can collect and aggregate Azure Monitor and Amazon CloudWatch log data from a variety of sources into a common data platform, where it can be used for analysis, visualization, alerting. Microsoft Power BI and Amazon Kibana transforms log data into rich visuals, sharing on the web and mobile devices. Log data can be analyzed with queries to quickly retrieve, consolidate, and analyze collected data. A Kusto query which is a read-only request was used to process data and return results. The request is stated in plain text, using a data-flow model. Gathering as much information as possible from multiple data sources will enable machines to predict future problems through artificial intelligence (AI) and automation. © *2021 Bull. Georg. Natl. Acad. Sci.*

Azure, cloud, AWS, services, monitoring, analysis, visualization

Data logging is the process of collecting and storing data over a period of time in order to analyze specific trends or record the data-based events of a system, network or IT environment. For logs to be useful, they require the following actions: Selecting useful information to store and archive; Ensuring the security and confidentiality of stored logs; Controlling the quality of log data by analysing and adding missing information to the logs; Monitoring of an application, is the ability to have a global view of an application at a given moment but also a history of past states. Monitoring is also important to detect any lack of server performance in real time [1].

Azure Monitor Views

Azure Monitor log contains different data types organized in records for different sets of properties for each type. Logs contain numeric values, such as Azure Monitor metrics, but usually contain textual

data with detailed descriptions. They differ from these metrics in that they depend on their structure and are often not collected at regular intervals. Telemetry data, such as events and traces, is stored in Azure Monitor logs, additional performance data, so that it can be combined for analysis [2,3].

A common type of journal entry is an event that is regularly collected. Events are created through an app or service and usually contain enough information to provide context.

Since data formats may vary, applications create their own journal using the required structure. Metrics stored in tabs to combine with other monitoring data to analyze trends and other data [4-7].

Log queries help us to fully leverage the value of the data collected in Azure Monitor Logs.

We use the Kusto query language to retrieve different types of log data from Azure Monitor.

Below examples of the log queris are given:

1. // Computers availability today

```
Heartbeat
| summarize count(ComputerIP) by bin(TimeGenerated, 1h)
| render timechart
```

2. // Usage by data types

```
Usage
| summarize count_per_type=count() by DataType
| sort by count_per_type desc
| render piechart
```

The amount of logs reported for each data type as a chart in Microsoft Azure Portal [8].

We have:

- Rich visualizations for log data.
- Integrates into Azure Monitor management model with workspaces and monitoring solutions.
- Filters for custom parameters.

Limitations:

- Supports logs but not metrics.
- No personal views. Available to all users with access to the workspace.
- No automatic refresh.
- Limited layout options.
- No support for querying across multiple workspaces or Application Insights applications.

Amazon Cloud Watch Views

Amazon EC2 (Elastic Compute Cloud) sends metrics to Amazon CloudWatch. CloudWatch Logs enables us to centralize the logs from all of systems, applications, and AWS services. CloudWatch log contains different data types organized in records for different sets of properties for each type. Logs contain numeric values, such as metrics from all AWS services, but usually contain textual data with detailed descriptions. We can see logs on the Amazon CloudWatch dashboards, views are customizable and with CloudWatch dashboards we can create customized views of the metrics and alarms for your AWS resources. We can focus on a particular services and resources. Telemetry data, such as events and traces, is stored in CloudWatch logs, additional performance data, so that it can be combined for analysis.

A common type of journal entry is an event that is regularly collected (By default, each data point covers the 5 minutes that follow the start time of activity for the instance). If we've enabled detailed monitoring, each data point covers the next minute of activity from the start time. We send our own custom metrics to CloudWatch. Events are created through an app or service and usually contain enough information to provide context.

Since data formats may vary, applications create their journal using the required structure. Metrics stored in tabs to combine with other monitoring data to analyze trends and other data [9].

Log queries help us to fully leverage the value of the data collected in CloudWatch Logs. The log queries examples are given below:

```
stats count(srcAddr) as IP by loggingTime, bin(1h)
```

Power BI Dashboards

To import data from a Log Analytics workspace in Azure Monitor into Power BI, a dataset was created in Power BI based on a log query in Azure Monitor. The query is run each time the dataset is refreshed. You can then build Power BI reports that use data from the dataset. To create the dataset in Power BI, we export our query from Log Analytics to Power Query language, then use this to create a query in Power BI Desktop and publish it to Power BI as a dataset. One of the features of Power BI Service is usage metrics report on a dashboard or report. The usage metrics report will give an analysis of how many times the content is viewed or share through which platforms and by which users [9].

So resourceful import the results of a log query into a Power BI dataset.

Microsoft Power BI Desktop has various icons to represent different visualizations (Fig.1). Depending on what we wish to display, we tick the checkbox for a particular data field, and then choose a chart type from the right pane.

In Power BI model we combine data from different sources [10,11].

Now we use **Power BI Desktop** to create reports, then publish those reports to the Power BI service, where we can view reports and dashboards.

Conclusion

Microsoft cloud services, such as Azure Monitor and Power BI and Amazon Web Services, such as Amazon CloudWatch and Kibana take advantage of its features such as combining data from different sources and sharing reports on the web and mobile devices. Power BI give us rich visualizations and reports for analysis of different sets of log data. After the initial import, the dashboard and the reports continue to update daily. We can control the refresh schedule on the dataset.

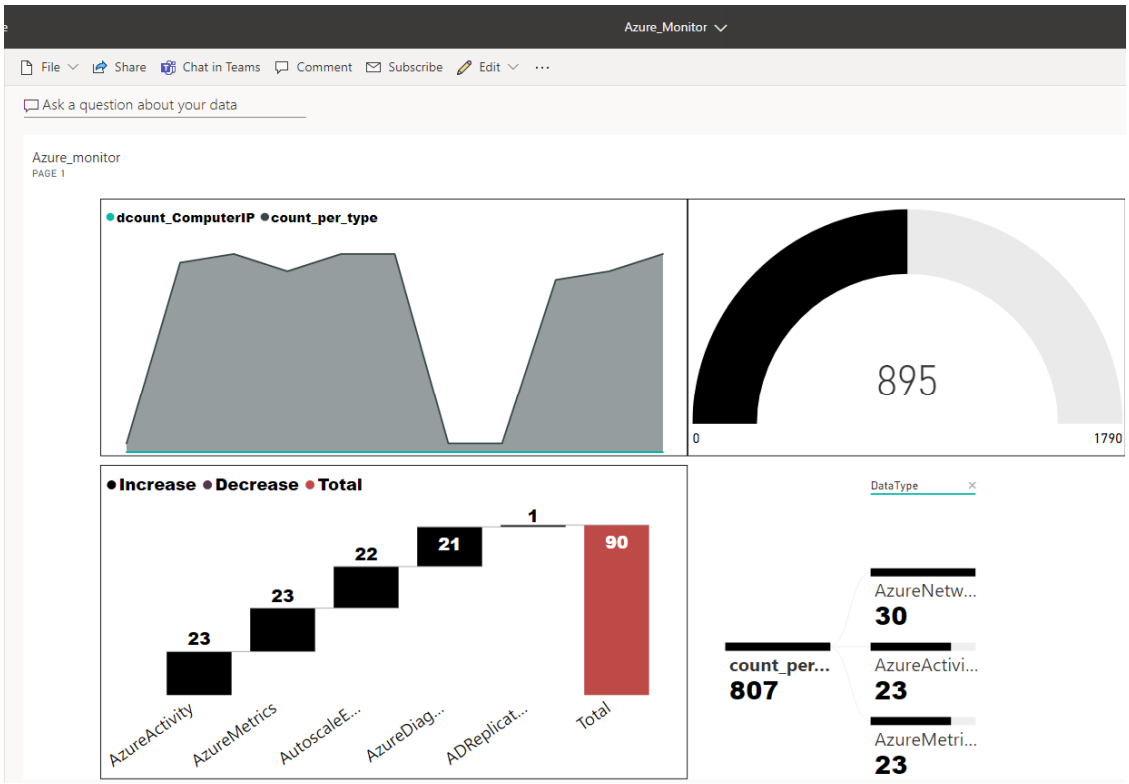

Fig. 1. Report in Power BI.

With the Azure Audit Logs content pack for Power BI, we can easily explore sensitive data using the initial set of metrics. Log intelligence can be defined as a method of log analysis that is powered by Artificial Intelligence (AI) and automation. Gathering as much information from many data sources will allow machines to predict future issues.

ინფორმატიკა

Log მონაცემების შეგროვება და ანალიზი ღრუბლოვანი სერვისებით

ო. შონია*, ნ. თოფურია*, კ. კულიჯანოვი**

*საქართველოს ტექნიკური უნივერსიტეტი, თბილისი, საქართველო
**საქართველოს ამერიკული უნივერსიტეტი, თბილისი, საქართველო

(წარმოდგენილია აკადემიის წევრის გ. ჩოგოვაძის მიერ)

თანამედროვე რთულ გამოთვლით გარემოში დაკვირვებადობის მისაღწევად, რომელშიც სრულდება განაწილებული პროგრამები, რომლებიც ეყრდნობიან ქლაუდის (ღრუბლის) და ადგილობრივ სერვისებს, აუცილებელია ოპერაციული მონაცემების შეგროვება თითოეული დონიდან და განაწილებული სისტემის თითოეული კომპონენტიდან. ძალზედ მნიშვნელოვანია ამ მონაცემების ღრმა ანალიზის ჩატარება და მისი კონსოლიდირება ერთიანი მინის პანელში, შეხედულების განსხვავებული რაკურსით, იმისათვის, რომ უზრუნველყოფილ იქნეს მხარეთა დაინტერესება ორგანიზაციაში. სტატიაში წარმოდგენილია Microsoft-ის ქლაუდის (ღრუბლის) მონაცემთა ჟურნალების მონიტორინგის სერვისები, ისეთი, როგორიცაა Azure Monitor და Power BI და Amazon Web Services, Amazon CloudWatch და Kibana. ამ სერვისების საფუძველზე ჩვენ შესაძლებლობა გვეძლევა უზრუნველვყოთ Amazon CloudWatch მონაცემთა ჟურნალის შეგროვება სხვადასხვა წყაროდან და შეჯამება მონაცემთა საერთო პლატფორმაში, შეძლებისდაგვარად მათი გამოყენება ანალიზისთვის, ვიზუალიზაციისა და შეტყობინებისათვის. Microsoft Power BI და Amazon Kibana გარდაქმნიან ჟურნალების მონაცემებს მდიდარ ვიზუალურ ეფექტებად, ინტერნეტსა და მობილურ მოწყობილობებში საერთო წვდომის უზრუნველყოფით. ჟურნალის მონაცემების ანალიზი შესაძლებელია მოთხოვნის მეშვეობით, მათი სწრაფი მობიებისთვის, კონსოლიდაციისა და ანალიზისთვის. Kusto მოთხოვნა, რომელიც წარმოადგენს მოთხოვნას მხოლოდ წაკითხვისთვის, გამოიყენება მონაცემთა დამუშავებისა და შედეგების დაბრუნებისთვის. მოთხოვნა სრულდება უბრალო ტექს-

ტით, მონაცემთა ნაკადის მოდელის გამოყენებით. მონაცემთა სხვადასხვა წყაროდან რაც შეიძლება მეტი ინფორმაციის შეგროვება საშუალებას აძლევს მანქანებს, მოახდინონ მომავალი პრობლემების პროგნოზირება ხელოვნური ინტელექტის (AI) და ავტომატიზაციის გამოყენებით.

REFERENCES

1. Shonia O., Kartvelisvili I., Beridze Z., Didmanidze I., Kolbaia L. (2017) Automatized design of the logic and structured process of wireless local area networks monitoring, *Bull. Georg. Natl. Acad. Sci.,* **11**(2): 22–28.
2. Shonia O., Kartvelishvili I. (2013) Algorithm of raising the security of routing of wireless local networks. *Georgian International Journal of Science, Technology and Medicine,* **5** (3/4): 239.
3. Prangishvili A., Shonia O., Rodonaia I., Rodonaia V. (2013) Formal security modeling in autonomic cloud computing environment. WSEAS/NAUN International Conferences, Valencia, Spain.
4. Prangishvili A., Shonia O., Rodonaia I., Mousa M. (2014) Formal verification in autonomic component ensembles Wseas/Naun International Conferences, Salerno, Italy.
5. Shonia O., Qartvelishvili I., Kolbaia L. (2014) Visualization and analysis inter-communication of normative-legal documents, *Georgian International Journal of Science, Technology and Medicine,* **6** (1): 67.
6. Prangishvili A., Prokopyev l., Shonia O. (2007) Modeling of decision making support system in conflicts control, *Bull. Georg. Natl. Acad. Sci.,***175** (4):87-92.
7. Nachkebia D., Shonia O., Kaishauri T. (2017) Code injection techniques into a remote process and its countermeasures, Information and Computer Technology, Modeling and Control: *Proceedings of the International Scientific Conference* Devoted to the 85th Anniversary of Academician I. V. Prangishvili, pp. 349–360.
8. Chogovadze G., Surguladze G., Topuria N., Archvadze N. (2020) Implementation of a prediction model with cloud services. *Bull. Georg. Natl. Acad. Sci.,* **14**(3): 29–35.
9. Lominadze T., Topuria N. (2017) Database realization for the corporation web-portal. Information and Computer Technology, Modeling and Control. *Proceedings of the International Scientific Conference Devoted to the 85th Anniversary of Academician I. V. Prangishvili,* Chapter 21: 227-234.
10. Katamadze S., Topuria N. (2018) Instant payment system business model and technical description. *Computer Sciences and Telecommunications,* 1(53). http://gesj.internetacademy.org.ge/en/list_aut_artic_en.php?b_sec=comp&list_aut=2788
11. Chogovadze G., Surguladze G., Topuria N., Gavardashvili A., Namchevadze T. (2018) Computer-aided design of the information ecosystem for monitoring of the Black Sea water resources. *Bull. Georg. Natl. Acad. Sci.* **12**(2): 10-26.

Received June, 2021