International Journal of Science and Research (IJSR)
ISSN: 2319-7064
SJIF (2019): 7.583

Elementary Monitoring Solution for Microsoft Azure Workloads

Sonali Mishra

Information Technology Analyst, Tata Consultancy Services

Abstract: ***In simple words "Monitoring" refers to a concept where any company/project maintain regular surveillance over their technical set-up. All the frameworks and technologies have different ways to implement this solution. This paper is basically focused on monitoring solution for azure native workloads, what/how should a standard set up looks like to cover end to end monitoring concept. Also this paper touch upon different key azure services required to do this set-up.***

Keywords: Microsoft Azure, Monitoring, Traceability, Logs, Alerts.

1. Introduction

Monitoring is a process which is must for any technical project. All the frameworks and technologies which are there in market need to have this set up for their system to continuously monitor the health of their system and in case to roll out or to troubleshoot any issues/root cause in case there is a system breakdown at given point of time. This paper is focused upon how a standard monitoring solution looks like for azure platform, how this monitoring system works, how logs are been captured, how performance of complete system can be checked upon and how alerting mechanism can be set up for the notification purpose and what are the different services involved to have this system in place.

Below is the standard generalized set up for the monitoring in azure, solution explained in detail in other section of the paper.

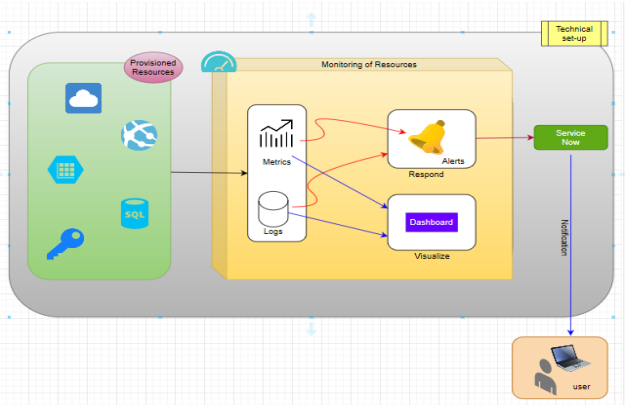

Figure 1

Here in (Figure 1), it shows a basic technical set up which consist of number of azure service for example: App service, App service plan, Database, key vault, blob storage. To capture complete end to end monitoring for all these services- logs and metrics are the two important things which need to be captured for all the respective services which your system composed of. Now to capture the response of logs and metrics there should be an alerting mechanism in place to capture if in case there are some unpredictable scenario, for example if your system deployed in app service starts giving 404.And this alerting mechanism should be designed in such a way so as to send proper notification via email or incidents to the end user or the developer. Also in order to have a good visualization for complete set up azure dashboard is a service which plays very important role to provide this feature.

2. Methods/Approach

To achieve this complete monitoring set up for azure platform below are the must have process/mechanism should be there in place as to collect required evidences for the later stage of troubleshooting.

a) Logging mechanism

Logging is process where we capture all the required logs of different services which are part of our complete technical stack. Logs can be of different kind to for ex: infra, application and security logs.

For azure platform "Azure Monitor logs" is the answer for logging set up to be done.

Azure monitor logs collect and organize logs. All the logs of different logs which are part of your technical stack can be accumulated at one single workspace called "Log Analytics workspace" which can be queried later with "Kusto query language" to retrieve specific set of data or to perform any data analysis over the data captured in logs. This workspace consist of number of tables to bifurcate logs of different kind in different tables. [1]

Below are the example of some standard table present in Log analytics workspace for capturing different kind of logs

- Azure Diagnostic
- Azure Activity
- Azure Metric

How these logging system is enabled:
For each of azure service there is a capability to enable logging system called as: "Diagnostic setting" which once enabled will automatically started sending data to attached log analytics workspace.

Significance of collecting azure logging data:

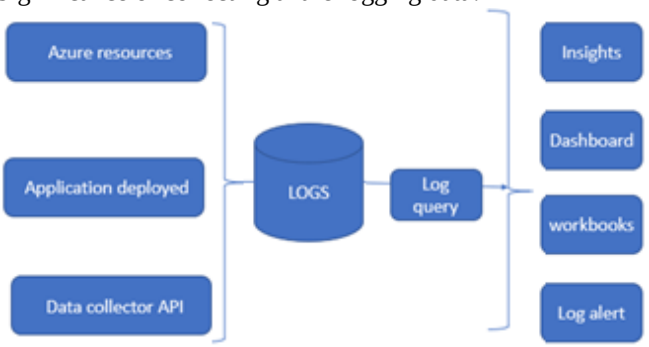

Figure 2

- Analyze : Logs are important to analyze working of your system.
- Alert: Plays important role while setting conditions for alerting mechanism.
- Visualize: Required log data can be queried and pinned to dashboard and workbook to get good visualization at single location.

b) **Metrics collection mechanisms:**

Metrics are nothing but numerical values that describe some aspect/characteristics of services at a particular time which counts for performance of your system. For example Response time of your deployed application. For Azure platform "Azure Monitor metrics" is a feature of Azure monitor that collect metrics from different resources part of your technical stack. And these values are collected at regular interval into a time series database.[2]

Example of basic metrics to be captured using azure monitor metrics for some resources:

- For AppService: Response time, health check status, http 2xx/4xx/5xx count.
- For Database :failed connection count, cpu percentage, deadlock count
- For Key vault: Availability of vault, API latency, unauthorized access.
- For Application gateway: health of backend pools, healthy host count.

Significance of collecting azure metrics data:

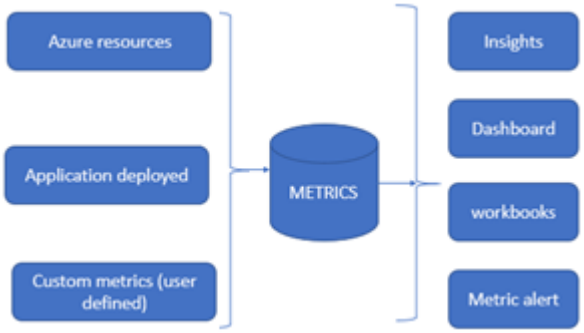

Figure 3

Analyze : Metrics are important to analyze performance of your system.

Alert: Plays important role while setting conditions for alerting mechanism.

Visualize: Can be visualize via Dashboards and workbook service of azure.

c) Alerting mechanism

Alerting mechanism is a process which is used to notify respective end user/developer if in case your system doesn't work as expected. There are ways to set up alerting mechanism in azure, based on that user will get notified via email or incident. Below is the basic alerting set up to be used for azure resources : [3]

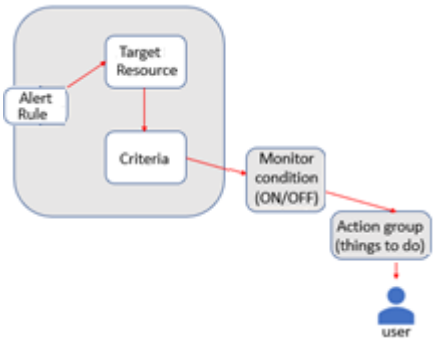

Figure 4

As per above Figure 4 alerting mechanism consist of an alert rule which composed of two important parts – Target resource on which alert should act and the criteria/condition when met alert should get fired.

Next is about the Monitor condition tells if your alert is enabled or disabled (ON/OFF).

Last but not least is the Action group which is required to set the action to be taken to notify the end user when alert got fired. There can be several ways can be used for notification purpose for ex : email, SMS, service now incident.

3. Conclusion

This paper tried to cover elementary monitoring set up on azure. The different service of azure to be used to have this capability enabled for any project based on azure platform. This basic knowledge can be used as a kick start for anyone who is new to azure framework and wanted to have this monitoring solution.

References

[1] https://docs.microsoft.com/en-us/azure/azure-monitor/logs/data-platform-logs
[2] https://docs.microsoft.com/en-us/azure/azure-monitor/essentials/data-platform-metrics
[3] https://docs.microsoft.com/en-us/azure/azure-monitor/alerts/alerts-overview

Author Profile

Sonali Mishra, Information Technology Analyst, Tata Consultancy Services. Working as an Azure DevOps Engineer.