Data Monitoring within Integrated Systems

Abstract

This paper aims to determine how analytics are used to assess the performance of systems. Accurate assessments of a system require analytics from an accurate and updated representation of that system. This accurate representation is gained by establishing a framework that supports continual monitoring and analysis and produces the information needed for decision makers to improve the system. Effective continual monitoring includes an understanding of the key components which support critical processes, setting specific performance goals that align with desired analytics, and measuring the key performance indicators (KPIs) that directly influence those goals. We examine how an organization leveraged network monitoring to enhance system performance and how cyber monitoring is used to gain insight into system security. We also address the increasing number of casualty reports (CASREPs) observed by the Department of Defense (DoD) and suggest ways to decrease this number using informative monitoring. Finally, we present common monitoring tools used to gather data relevant to system performance.

Performance Monitoring Framework

There are many frameworks available today that support the measuring and gathering of data for analytics. Common frameworks can include Information Technology Infrastructure Library (ITIL)[1], Fault-management, Configuration, Accounting, Performance (FCAPS)[2], and Business Process Framework (eTOM)[3]. The benefits of implementing a common framework are to establish a unified language, culture, and process for effectively leveraging and maintaining technology for the purpose of enhancing system performance. Common performance essentials include:

- prioritized ticket monitoring;
- maintaining a knowledge base of continuously updated and accessible documentation;
- frequent reporting of incidents, causes, and resolutions; and
- monitoring of infrastructure and system performance [4].

Monitoring and maintaining these essential functions support the overall health of a system and guide analytics for decision making. Associated with each of these activities are specific performance goals that produces several key performance indicators that guide the data collection needed to perform analysis.

Data Collection

Defining what data is being captured and what the data is measured against is critical when considering data collection. Monitoring devices only start to be effective when decision makers first identify critical components and services within the system, set performance goals and define the desired outcomes that will be gained from data analytics, and develop key performance indicators (KPIs) that can be used to measure the improvement or degradation of performance.

Identify Critical Components

For commercial organizations, the criticality of the business process often correlates to the amount revenue produced by that business process, confidentiality of the information it processes or stores, its role in negotiating contracts, and its communication with customers, vendors, investors, or employees [5]. Each of these factors determines the value each business process has within a company. Similarly, a defense system's criticality is also determined by a set of factors that identify the critical functions and assets that have the potential to cause significant threat and degradation to the mission if compromised. Identifying these critical components focuses attention to the areas with the greatest need for information gathering to ensure resiliency and mission success.

Set Performance Goals

A performance objective precedes effective performance monitoring. Gathering data about a system means little to decision makers until that data is analyzed against specific performance goals. Properly defined goals have the following characteristics:

- **Repeatable**: to facilitate comparisons
- **Observable**: so that performance can be analyzed and understood
- **Portable**: to allow benchmarking against competitors and across different product releases
- **Easily presented**: so that everyone can understand the results
- **Realistic**: so that measurements reflect customer-experienced realities
- **Runnable**: so that developers can quickly test changes [6]

The goals describe what is being tested, the limiting factor(s), any variances that might affect the result, and the conclusions that can be drawn [6]. For example, the National Ignition Facility (NIF) sought to enhance their performance by introducing a new policy concerning the timeliness of issue tracking [7]. The time required to resolve an issue was identified as a limiting factor that was addressed within the new policy. Once this limiting factor was identified, it could then be observed to determine the achievement or non-achievement of the goal.

Determine Key Performance Indicators

With such goals defined, key performance indicators can be identified. These indicators are quantitative metrics that have a direct correlation to the achievement or non-achievement of the

specified performance goals [10]. Examples of KPIs include indicators such as CPU load, memory utilization, and swap use.

Data Monitoring

There are various metrics that can be measured within a system. The overall goal, however, is to minimize downtime, enhance current capabilities, and prioritize the available resources accordingly. These goals are often attained by using monitoring capabilities to derive mean time between failures and performance degradation of components, manage network incidents, and provide metrics-based decision making. Such capabilities provide the ability to identify parts that need of maintenance or repair before a situation escalates resulting in downtime and to report on system metrics that can be used to enhance system performance. The following examples illustrate how an organization can use various metrics to attain specific performance goals.

Network Monitoring

Since 2014, the National Ignition Facility (NIF), the "world's largest and most energetic laser experimental facility," has used Splunk, a commercial product, to collect, aggregate, and manage computer log files into a centralized, indexed database with search, data processing, and visualization capabilities [7]. In leveraging Splunk's capabilities, the NIF has incorporated several system enhancements that have increased its operations.

Enhance System Performance

To monitor their operating system performance, NIF used Oracle Enterprise Manager (OEM) to house all raw performance data and used OEM as a data source for Splunk to collate and display these performance metrics through dashboards [7]. After using Splunk to categorize their large number of hosts into groups of comparable hosts, such as framework servers, supervisory applications, front-end processors, and operating consoles, a dashboard conveys an accurate representation of performance. Using this dashboard helped identify abnormalities and enabled NIF to remediate an issue that caused three outlying x-ray imaging systems to be exceed their memory capacity [7]. They were able to identify and diffuse the situation before it could escalate and cause lasting damage to the system.

Inform Acquisition Processes

By continuing to leverage Splunk capabilities and collecting data logs of their critical components, the NIF was able to identify indicators of their critical components and establish criteria for identifying both healthy and degrading devices. Doing so enabled NIF to prioritize resources and begin the replacement processes as necessary with minimal downtime [7].

Manage processes

NIF leveraged Splunk's data indexing capabilities by capturing data of their routine experiments [7]. The indexed data allowed for a multi-level understanding of each experiment, expressing the time it took to complete each experiment's key state transitions, and the components responsible for the elapsed time [7]. The levels of detail enabled operators to analyze a high-level

view of multiple experiments at once as well as identify specific device abnormalities within an experiment's critical path.

Cyber Monitoring

Unfortunately, the value of cyber monitoring is too often not fully understood until an attack has targeted an unprepared system resulting in devastating effects. Various tools can be used to avoid these effects. Among these tools include discovery scans and trend analysis.

Discovery Scans

Discovery scans are used to reveal known vulnerabilities within the system; allowing operators to patch and prioritize remediation. In 2016, a federal government civilian agency was consistently targeted by nation state actors. The agency introduced RedSeal, a network discovery and vulnerability management tool, into their enterprise. The tool discovered the agency's active network and integrated the vulnerability scan findings to significantly improve their remediation strategy, increasing work efficiency and reducing risk to the system [8].

Trend Analysis

Another method includes using trend analysis of historical cyber incidents. The Navy Cyber Defense Operations Command (NCDOC) is a command that uses a standard to actively collect, analyze, and report on various cyber incidents throughout the Navy [9]. Information regarding these incidents is gathered from various platforms then aggregated to detect patterns of re-occurring incidents. The patterns are communicated to the fleet to allow proactive development of remediation or mitigation strategies and effective response actions [11]. Capturing these incidents provides a means to decrease potential downtime and increases opportunities to safeguard critical assets.

Current Challenges

According to a U.S. congressional report, a known challenge within the Navy is managing an increasing influx of Navy casualty reports (CASREPs), which have doubled from the year 2009 to 2014 [12]. A major contributor to this issue includes the lack of an integrated database, which maintains a complete representation of system equipment data [14]. Lacking a complete representation of the system decreases awareness of maintenance needs, currently driving life-cycle maintenance costs and unplanned maintenance time [14]. Using an MBSE approach, a digital twin can be used to depict an integrated representation of the complete system [13]. With an integrated database to house monitored KPIs that contribute to the health of critical devices, which potentially demand a CASREP, the Navy can decrease both maintenance costs and time. The KPIs can be collected, analyzed, and used by decision makers to prioritize and properly schedule maintenance needs, minimizing system downtime.

Summary

A framework centered on system performance continually affirms the value of quantitative data that supports the system performance goals. Quantitative data is gathered by using tools to

measure and aggregate the associated KPIs of each performance goal. Figure 1 describes several monitoring tools that are currently being used to collect several KPIs. Identifying performance goals and associated KPIs directs proper aggregation of the data, which is necessary to find trends and abnormalities within the system. Decision makers can then be equipped with the information necessary to understand a system's health and allocate resources appropriately to provide the necessary system sustainment and maintenance needs.

Tool	Support	User Interface	Alerts	Web or mobile client	Auto-mation	OS Support	Strengths
Nagios	Active support community	Improved Web GUI†	Email, SMS, custom	Web interface	Yes†	Linus, Unix, Windows via proxy agent	Flexible and highly configurable, robust, and reliable
Zabbix	Active support community, email, forums, help desk, phone, wiki	Well-designed Web GUI	Email, SMS, custom	Web interface	Yes with API	Windows, Mac, Linux, Unix	Flexibility to organize monitoring data, configurability, scalability
Hyperic	Support community, email, help desk	Good Web interface	Email, SMS	Web interface	Yes†	Windows, Mac, Linux, Unix	Native management for Unix, Linux, Windows, and Mac scalability
SolarWinds	Active support community, email, forums, help desk, phone	Excellent GUI	Email, custom	Web interface, mobile	Yes	Windows, Mac, Linux, Unix	Quick and easy deployment, affordability, native support for VMware
ManageEngine OpManager	Email, forums, help desk	Atypical UI that is hard to navigate	Email, custom	Web interface, mobile	Yes	Windows, Mac, Linux, Unix	Great feature set
HP Operations Manager	Forums, help desk, webinars	Good Web interface	Email, SMS, custom	Web interface, mobile	Yes	Windows, Linux, Unix	Integration with other products from the same company; integration with HPIC, which can integrate with SCCM or SCOM*
IBM Tivoli	Email, forums, help desk	Good Web interface	Email, SMS	Web interface	Yes	Windows, Linux, Unix	Automatic analysis and repair, efficient where many resources must be monitored
WhatsUp Gold	Phone, email, forum	Clumsy interface	Email, SMS, sound	Web interface	Yes	Windows	Easy setup and network discovery, great feature set

* SMS is short message service, HPIC is HP insight Control, SCCM is System Center Operations Manager, and SCOM is System Center Operations manager.
† Only in the paid version.

Figure 1 Eight popular IT-monitoring tools of 2015 [15]

References

1. ITIL® Processes & Best Practices. (2018). Retrieved from http://www.bmc.com/guides/itil-introduction.html
2. Rouse, M. (n.d.). What is FCAPS (fault-management, configuration, accounting, performance, and security)? - Definition from WhatIs.com. Retrieved from https://searchnetworking.techtarget.com/definition/FCAPS
3. Tmforum. (2014, August 20). Business Process Framework (eTOM). Retrieved from https://www.tmforum.org/business-process-framework/
4. Chavan, S. (2016, December 24). Best Practices for Building Network Operations Centers
5. Lyons, L. B., IV. (2006). Preparing For A Disaster: Determining the Essential Functions That Should Be Up First. SANS Institute.
6. Gregg, B. (2014). Systems performance: Enterprise and the cloud. Upper Saddle River, NJ: Prentice Hall.
7. Fedorov, M. A., Adams, P., Brunton, G. K., Fishler, B. T., Flegel, M. S., Wilhelmsen, K. C., & Wilson, E. F. (2018). Leveraging Splunk for Control System Monitoring and Management. Geneva, Switzerland: JACoW
8. Federal Civilian Agency Saves the Day [Review]. (2018, February). RedSeal.
9. US Fleet Forces Command NCDOC. (n.d.). Retrieved from https://www.public.navy.mil/fltfor/ncdoc/Pages/default.aspx
10. Weber, A., & Thomas, R. (2005). Key Performance Indicators, Measuring and Managing the Maintenance Function. Ivara Corporation.
11. U.S., Chairman of the Joint Chiefs of Staff Manual. (2012). CJCSM 6510.01B.
12. U.S. Cong. (2015). Navy force structure: Sustainable plan and comprehensive assessment needed to mitigate long-term risks to ships assigned to overseas homeports: Report to congressional committees (P. J. H., S. Wren, J. Ashley, S. Banovac, J. Landesman, A. Lesser, et al., Authors) [Cong. Rept. ADA618348].
13. G2 Ops Inc. (2018). Model-Based Systems Engineering (MBSE).
14. Martin, B., Yardley, R. J., Pardue, P., Tannehill, B., Westerman, E., & Duke, J. (2018). APPROACH TO LIFE-CYCLE MANAGEMENT OF SHIPBOARD EQUIPMENT. Santa Monica, CA: RAND CORPORATION, RR-2510-NAVY.
15. Hernantes, J., Gallardo, G., & Serrano, N. (2015). IT Infrastructure-Monitoring Tools. IEEE Software, 32(4), 88-93. doi:10.1109/ms.2015.96