UDC 681.5

Control system for automated operation of a globally distributed telecommunications network

V.V. Efimov*, D.A. Shchemelinin, Ph.D.†

* *St. Petersburg Polytechnic University, Polytekhnicheskaya 29, St. Petersburg, Russia, 195251*

† *RingCentral Inc., San Mateo, CA, USA, 94404*

Abstract. A globally distributed computing system providing a telecommunications cloud service under 99.999% SLA usually consists of a set of components, designed to execute a dedicated function, such as user authorisation, data storage, data analysis, media conversion, etc. Total number of remote servers is up to tens of thousands. Such complex service requires efficient operations tools to run Event Management, Incident Management, Change Management, Problem Management. This paper provides study on control system for automated operation of a globally distributed telecommunications network using well-known tools such as monitoring tool, log collector, configuration management database and other as sensors, controllers and actuators.

Keywords: cloud service, telecommunications network, configuration management, CMDB, control system, automation.

1. Introduction

An efficient operation of a globally distributed computing system and resource planning requires specialised software tools, such as a tool for automated resources allocation (compute, storage, network bandwidth), service restoration [4], deployment of software updates on all layers of the technology stack (firmware, OS, application).

Thus, the specialised software tools are usually divided into two categories: a) business applications aimed for enterprise resource planning (ERP tools) and b) information system operation tools, designed to execute following functions: 1. Deployment of software updates as part of SDLC, including critical security patches; 2. Control and monitoring of computing system capacity [5]; 3. Update of operating systems, running both on virtual and hardware machines; 4. Data and virtual machines backup and restoration in case of system failure; 5. Authentication, authorisation and access control

It is a common practice among IT companies providing cloud computing services to use specialised monitoring and management software. It significantly reduces the number of manual repetative tasks, reduces number of incidents cases by human errors, therefore, making operation of a cloud service more reliable. [1]

The analysis of specialised software tools for automated operation of a cloud computing system in big IT companies [2] showed that in most cases the implementation of such tools was 'ad-hoc', was done with no

strategy, which led to the situation, when a company had to deal with big number of heterogeneous software tools with incompatible API, which blocked standartization of operation processes.

To prevent such a situation, the control system for automated operation of a globally distributed computing system is introduced as a universal, vendor independent solution.

2. Main section

A typical information system consists of computing units and informational links with flows of data. Besides this, each information system has its function and clients using its service under service level agreement. A monitoring system is used to achieve the service level agreement.

Implementation of a specialised monitoring software tool is always considered a complex project, part of general automation of operations. It should be considered that there are several types of data, needed to be collected for further analysis, independent of monitoring system used:

- Health data from remote computing units, including CPU utilisation, network availability, business applications status
- Application activity log, including error log
- Versions of operating systems, third-party software and business applications, deployed in each computing unit and their comparison with planned values

Fig. 1 shows the introduced control system, which consists of well-known components.

Sensors:

- Health data and log collectors are scalable components with function to collect and generalise data from remote monitoring agents, located in virtual machines of any type. The collector of remote data should garantee acquisition of data and its delivery to centralised monitoring system.
- Time-series database stores full array of data from sensors and is aimed to serve queries for historical data in real time

Actuators:

- Configuration Management Database (CMDB) has data on system topology (units and links) as well as unit operation statuses
- Automated Deployment System (ADS) deploys additional computing units for capacity extension and during ongoing maintenance

Controllers are based on ITIL best practices [6]:

- Change Management - assures a change is reviewed, approved and communicated to stakeholders
- Incident Management - minimises system impact through escalation and coordination of restoration activities
- Release Management - plan and schedule for roll-out of software updates as part of SDLC

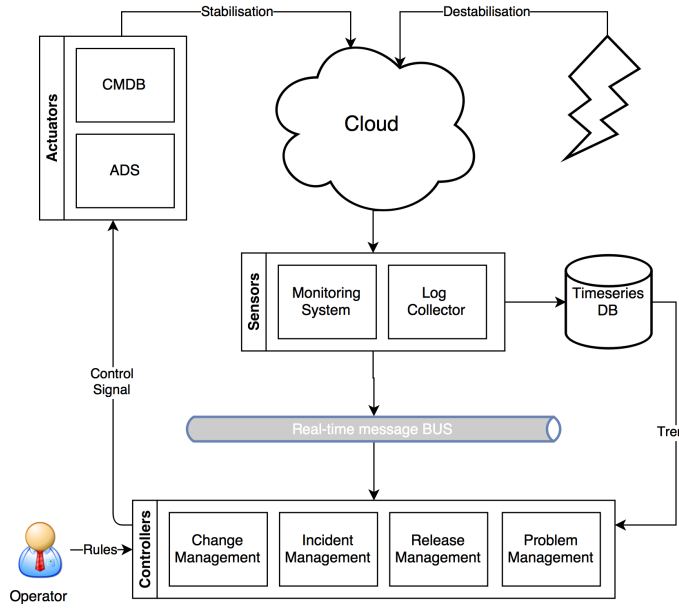

Figure 1. Control system for automated operation of globally distributed computing system

— Problem Management - prevents chronic problems from repeating through identification of the root cause, tracking of a permanent fix from development to roll-out to production

Operator configures controllers, providing machine-readable rules of operation.

In order to enable the above components to work together in the control system, following requirements have to be met:

— Sensors, including monitoring system are required to perform distributed data collection and processing from several nodes;
— Each specialised software tool has to have an API for integration with other tools;
— The tools need to use CMDB as a single authoritative point of data;
— The tools need to support software development lifecycle by supporting changes in the globally distributed computing system under operation, such as software updates, addition of new components, topology change;
— Scalability up to tens of thousands of remote hosts and hundreds of thousands of remote checks;

— Dynamic configuration of monitoring items including set up of thresholds;
— Anomaly detection based on historical monitoring data;
— Monitoring of globally distributed computing systems and geographical redundancy;

3. Conclusions

A universal, vendor independent control system for operation of globally distributed computing system was introduced. It uses well-known specialised software tools as its elements, introducing requirements to enable them to work as the system. This control system supports perspective control scenarios, which are currently under development, such as:

— Incident prediction based on dynamic performance patterns and response time measurements in different week days and time of a day;
— Fully automatic operation of a computing system due to ability to adopt to dynamic performance requirements;
— Visualisation of a computing system topology in real time to show dependencies between the system elements.

Acknowledgments

This work is implemented at and is partially supported by the International RingCentral Company [3]

References

1. *Martin Atzmueller, Samia Oussena, Thomas Roth-Berghofer* Enterprise Big Data Engineering, Analytics and Measurement. — IGI Global, 2016
2. *Kucherova K.N., Mescheryakov S. V., Schemelinin D.A.* Comparative analysis of monitoring systems for globally distributed computing systems. — System Analysis in Engineering and Control: XX international conference. — SPbSTU, 2016, p. 303-309 http://elib.spbstu.ru/dl/2/k16-18.pdf/download/k16-18.pdf
3. RingCentral Inc. http://ringcentral.com
4. *Ardulov Y., Mescheryakov S. V., Schemelinin D.A.* Monitoring and remediation of cloud services based on 4R approach — 41st International IT capacity and performance conference, San Antonio, 2015
5. *Mescheryakov S. V., Schemelinin D.A.* Capacity management of Java-based business applications running on virtualised environment — Annual international conference of the computer measurement group, 2013
6. ITIL Service Operations. https://ru.wikipedia.org/wiki/ITIL