

Research of virtualized log management system in communication dispatching center of power grid

Jianwen Ling*, and Yafei Luo

Guangzhou Power Supply Bureau, Guangdong Power Grid Co., Ltd. China Southern Power Grid, P.R. China

Keywords. Log, Log management, Log system, Virtualization.

Abstract. Logs happen every day. They record all kinds of events of current network and its management facilities. Communication dispatchers can use it to aware network or facility failures. In the purpose of improving awareness of communication network and its management facilities, this research is focusing on a log management system for different types of communication devices and network management servers. From log system architecture, to actual situations of log collection. Then, the distribution of system, from bare-metal servers to virtual machines. Most a virtualized log management system is deployed and tested in a dispatching center of power grid.

1 Introduction

Device and system logs provide a huge amount of information of current network and its management facilities. They record noteworthy events, such as network link down, device hardware failure, unauthorized login, but also trivial events, such as customer port up/down, network path switching, periodically system updates.

Currently, communication dispatchers monitor more than a dozen networks via different network management systems. In order to aware the network failure and dispatch maintainers promptly, communication dispatchers check every network management system periodically. They spent a large amount of time in differentiating system logs to find out whether there is a failure in those networks or management facilities.

With complete logs, communication dispatchers can analyze current status of the network, also backtrace the past status. In conjunction with several properly rulesets, machines can automatically reconstruct events, detect network failures, and aware system intrusions. Furtherly, provide guidance to communication dispatchers to draw up a strategy to settle such events.

* Corresponding author: lingjw@guangzhou.csg.cn

Hence, a log management system can effectively reduce communication dispatchers' checking time, aware emergence or major failures when such events occur. Comparing to bare-metal deployment, virtualization technology is introduced in the last.

2 System design

In this research, the log management system is design and implemented in four major modules, including log collection, log aggregation and storage, log analyzing, and log monitor.

2.1 Log collection module

This module is focusing on collecting logs from different varieties of communication devices and network management facilities. For different types of communication devices use different logging interfaces, this module supports syslog, SNMP (Simple Network Management Protocol), CORBA (Common Object Request Broker Architecture), etc. Also, this module supports IPMI (Intelligent Platform Management Interface) events, Windows and Linux logs in order to monitor the status of network management servers.

For security reasons, computers and networks are divided into the production control zone and the management information zone in power grid enterprises. Production control zone and management information zone are isolated by forward and reverse isolation devices. [1] Hence, log collection module should be deployed in both zones separately.

2.2 Log aggregation and storage module

Since logs collected from different devices and facilities have different formats, saving them directly is not suitable for fast searching and analyzing. This module not only saves the original logs, but transforms them into a uniform data table.

Several key information is included in the data table.

- (1) Event name, which can be extracted from alarm name or keywords in logs.
- (2) Event source, which helps identify the event occurred from which network, which device and which part of the device.
- (3) Event occurred time and resumed time, which helps analyzing related events and crucial to event monitoring and statistic.
- (4) Comments, for communication dispatchers to add memorandum and link such events to operation records, failure records, or scheduled records.

2.3 Log analyzing module

Tens of thousands of logs generate every day. It's impossible for communication dispatchers to check every log to find out emergence or major failures. This module automatically analyzes related logs generated in a short period of time.

For transmission network and data network devices, e.g., SDH/OTN network elements, routers, and switches, several network links down at the same time or in a very short period of time, and related hardware does not report any hardware failure, that probably means the optical fiber cable, which carrying such network links, is broken.

For network management facilities, e.g., Linux servers and Windows servers, remotely login event occurred without authorized maintenance operation records, that probably means the system is breached.

After analyzing related logs, this module can identify the root of those logs, additionally provides guidance to settle such events.

2.4 Log monitor module

This module provides root logs view, emergence and major alarm logs view, and original logs view of each network and facility separately. When root logs occurred, this module plays a warning sound to remind communication dispatchers.

Both B/S (Browser/Server) and C/S (Client/Server) structures are allowed in the management information zone in power grid enterprises, but B/S structure is not recommended in the production control zone. Hence, log monitor module is based on C/S structure.

3 Log reporting and collecting

According to the provisions, networks and servers are divided into two zones, the production control zone and the management information zone, in communication dispatching center of power grid. Furtherly, the production control zone is divided into the control area (security area I) and the non-control area (security area II), the management information zone is divided into security area III and security area IV.

The control area (security area I) and the non-control area (security area II) are under logical isolation. Systems and devices in different areas of the production control zone can connect through firewalls. The same logical isolation happens between security area III and security area IV.

However, systems and devices in the production control zone and the management information zone can only transfer text messages through isolation devices.

Currently, SDH/MSTP (Synchronous Digital Hierarchy/Multi-Service Transport Platform) optical transmission network, power dispatching data network, communication network for power distribution grid, etc. and their management systems are deployed in security area I. Communication power supply supervisory control system is deployed in security area II. Power integrated data network, unified communication network and their management systems are deployed in security area III. [2] Log management system collects logs from those devices and systems in different ways.

SDH/MSTP optical transmission network devices report event logs and alarms to management systems, and the optical transmission network management system provides a northbound interface using CORBA. Log management system should connect to the northbound interface to get logs reported by network management system.

Data network devices, e.g., routers and switches, can be configured to report every log through syslog and SNMP Trap. Just set syslog and SNMP Trap target to log management system, and most of logs can be collected. However, syslog and SNMP are running over UDP (User Datagram Protocol) but not TCP (Transmission Control Protocol), the data packets maybe lost in transmission. Log management system should periodically acquire full logs from data network devices' log buffer.

Linux server can be configured to report logs through syslog, or log management system acquire log files through SSH (Secure Shell Protocol).

Windows servers can use SCOM (System Center Operations Manager) or WEF (Windows Event Forwarding) to gather logs. However, both SCOM and WEF are mostly deployed on Windows Server, not suitable for a unified log management system. Therefore to get Windows Event Logs third-party agents, e.g., Evtsys (Eventlog to Syslog Utility by Purdue University), Rsyslog Windows Agent and NXLog

Logs of network management facilities, e.g., physical servers, can be acquired through IPMI interface.

After gathering logs in the production control zone, log collection module should forward all the logs to the log aggregation and storage module deployed in the management information zone through isolation devices. Then, logs can be processed in the management information zone only.

4 Virtualized deployment

As already stated in previous sections, one log collection module is deployed in the production control zone, and a log management system, including all four modules, is deployed in the management information zone. They can be deployed on bare-metal servers or virtual machines.

If log modules and system are deployed on bare-metal servers, those physical hosting devices are dedicated. All computing resources, including CPU, RAM and disk space, are exclusively used for log modules and system. Although bare-metal server provides high performance, there are two major disadvantages of this deployment way in real world.

Firstly, there are more than one hundred network management and security monitoring services in communication dispatching center of power grid. If each service or system occupies one bare-metal server, there is not enough space for such large number of servers in the data center of communication dispatching center. Furtherly, even though there are enough space, the power consumption is huge, and the UPS (Uninterruptible Power Source) would not provide long-enough run time.

Secondly, in the data center of communication dispatching center, all of the bare-metal servers are high performance servers, e.g., hundreds of CPU cores, several Terabytes of RAM. Such a log module or system will not cost so many resources. It will be a huge waste of investment using bare-metal servers for log module and system deployment.

On the contrary, deploying on virtual machines provides more benefits.

Firstly, virtualization saves space and power. One high performance server is capable of hosting dozens of virtual machines. In each security area, only three or four high performance servers can provide enough computing resources for all network management and security monitoring services, including log management system.

Secondly, virtualization saves time. A new deployment of virtual machine only takes a few minutes, when ordering and setting up a new bare-metal server will take days. When hardware or software failure occurred, virtual machines protected with High Availability or Fault Tolerance can recover in minutes even seconds. However, it will take hours or even days for bare-metal servers.

Lastly, virtualization helps maintainers. When computing resources of a service is not enough, it only takes seconds for maintainers to assign more vCPU, RAM or disk space to the virtual machine on which running such service. But if the service is running on a bare-metal server, it will take hours.

In summary, it's better to deploy a log collection module on virtual machine in the production control zone and a log management system on virtual machine in the management information zone.

5 Summary

In this article, the need of communication dispatchers was identified. Then the architecture of a log management system was proposed, and log collecting methods were introduced. The practical application of a virtualized log management system was found. The reliability

and stability of this system are tested. And it has been running in a communication dispatching center of power grid for more than two years.

References

1. Standardization Administration of the People's Republic of China, *Guidelines of cyber security protection for electric power system supervision and control*, **GB/T 36572-2018**, (2018)
2. China Southern Power Grid, *Technical specification for communication network management and service application system of CSG*, **Q/CSG 1204037-2018**, (2018)