TEST Engineering & Management

November-December 2019
ISSN: 0193-4120 Page No. 4095 - 4100

Using SPLUNK to Implement SIEM Capabilities

Remaz Alawaji
College of Engineering,
EFFAT University
AnNazlah Al Yamaniyyah, Jeddah, 22332, Saudi Arabia
rzalawaji@effatuniversity.
edu.sa

Dalal Alshiekhi
College of Engineering,
EFFAT University
AnNazlah Al Yamaniyyah, Jeddah, 22332, Saudi Arabia
daalshiekhi@effatuniversity.
edu.sa

Adel M. Ilahi
College of Engineering,
EFFAT University
AnNazlah Al Yamaniyyah, Jeddah, 22332, Saudi Arabia
aiilahi@effatuniversity.edu.sa

Article Info
Volume 81
Page Number: 4095 - 4100
Publication Issue:
November-December 2019

Article History
Article Received: *5 March 2019*
Revised: *18 May 2019*
Accepted: *24 September 2019*
Publication: *19 December 2019*

Abstract:

The data in logs may differ in general helpfulness, yet before one can infer much value out of them, they initially should be empowered, at that point can transport and eventually stored. SIEM items normally give a large number of the highlights required for log administration, but add event-reduction, cautioning and continuous examination abilities. They give the layer of innovation that enables to one to state with certainty that is logs being accumulated as well as being evaluated. Splunk security solutions not just meet the new criteria for the present SIEM, yet in addition deliver security analytics capabilities, giving the significant setting and visual bits of knowledge that assistance security groups to settle on quicker and more intelligent security choices. Splunk software can be utilized to work security operations centers and support the full scope of Information Security Operations including standardized evaluation, monitoring. Splunk also support for SIEM utilize cases likewise, detect known and obscure dangers, and explore dangers. This study utilized Splunk to implement SIEM capabilities.

Keywords: *Security; SIEM; SPLUNK*

1. Introduction

As an article justified by Kavanagh et al. (2016), SIEM arrangements are frequently funded to address regulatory consistence detailing prerequisites, however, the company is utilizing this as a chance to convey SIEM technology that will enhance risk administration and occurrence reaction abilities [1]. According to Aguirre and Alonso (2012), numerous preventive security efforts indicate to protect networks from cyber intrusions [2]. These embraced measures can create a lot of data that ought to be stored and analyzed to enable responses to detected attacks. Security information and event managers (SIEMs) are fundamental for gathering the majority of a system's security-related data in a focal storehouse. This would then be able to give incline investigation and lead analysts to adopt appropriate actions. Van Der Aalst (2013) clarified that Business Process Management (BPM) is the propriety that joins knowledge from data technology and knowledge from administration sciences and applies this to operational business forms [3]. It has received significant consideration as of late because of its potential for sign can't expand profitability and sparing expense.

Di Sarno et al. (2016) argued that Security information and event management (SIEM) systems are progressively used to adapt to the security challenges associated with basic foundation assurance [4]. In any case, these systems have a few constraints. Upgraded security information and event management system that (I) settle clashes between security approaches; (ii) finds unauthorized information ways and suitably reconfigures organize gadgets; and (iii) gives an intrusion and fault-tolerant storage systems that guarantee the trustworthiness and non-forgeability of stored events.

SIEM gives the end user the ability to not only gathers data from heterogeneous sources, but also makes the data immutable from the perspective of the privileged user. In addition, it allows the user to look at events from both the past and real-time environments, thus fulfilling the role of both preventive and detective controls. This study aims to utilize Splunk software to cull information together from various sources under one platform and use the logs as both preventive and detective controls.

2. Methodology

2.1 Functional Requirements

1. Policies and procedures for the organization should address the preservation of original logs.
2. Organizations should endeavor to be adaptable since every system is extraordinary and will log distinctive amounts of information than different systems.
3. Organizations may wish to obtain duplicates of the first log documents, the concentrated log records, and deciphered log information. Holding logs for proof may include the utilization of various types of capacity and diverse procedures.
4. Applications should log and analyze the information that is of most noteworthy significance, and furthermore have non-compulsory suggestions for which different sorts and sources of information ought to be logged and analyzed if time and assets allow.
5. Organizations ought to consider implementing log management infrastructures that incorporate brought together log servers and log information stockpiling. When designing infrastructures, associations should anticipate both the present and future needs of the infrastructures and the individual log sources all through the organization.
6. Factors to consider in the design incorporate the volume of log information to be prepared, organize transfer speed, on the web and disconnected information stockpiling the security necessities for the information, and the time and assets required for staff to investigate the logs.
7. To guarantee that log administration for singular systems is performed viably all through the organization, the managers of those frameworks ought to get sufficient help. This ought to incorporate spreading data, providing training, and assigning purposes of

contact to answer questions, giving particular specialized direction, and making tools and documentation available.

8. The major log management operational processes which include configuring log sources, and performing should be detailed as shown in Figure 1.
9. Log analysis, starting reactions to distinguish occasions, and overseeing long haul stockpiling ought to end up some portion of the organization's process.
10. The administrator should Check for upgrades and patches to logging software, and acquire, testing, or deployment.
11. Guaranteeing that each logging host's clock is synced to a typical time source.
12. Reconfiguring logging as required in light of policy changes, technology changes, and different factors, Documenting and detailing irregularities in log settings, designs, and procedures.
13. Monitoring the logging status of all log sources.
14. The organization needs to keep the availability of their logs.
15. The organization has to determine its requirements and goals for implementing logging and monitoring logs to involve viable laws, regulations, and current organizational policies (Figure 2)
16. Recurrent audits are one approach to support that logging standards and guidelines are being followed after all through the organization.
17. Testing and validation can additionally guarantee that the policies and procedures in the log management process are being performed appropriately.
18. The organization can organize its objectives in view of adjusting the organization's reduction of risk with the time and resources expected to perform log management capacities.
19. The organization needs to make and maintain segments of a log management foundation and decide how these segments interact.
20. Create an infrastructure sufficiently powerful to deal with not just expected volumes of log data (Figure 3)
21. Documenting and reporting peculiarities in log settings, setups, and procedures.

2.2 Non-functional Requirements

1. Logs should be attentive to the truthfulness of each log source.
2. Logs necessity to be conserved from breaking of their confidentiality and integrity, and they contain records of system and network security.

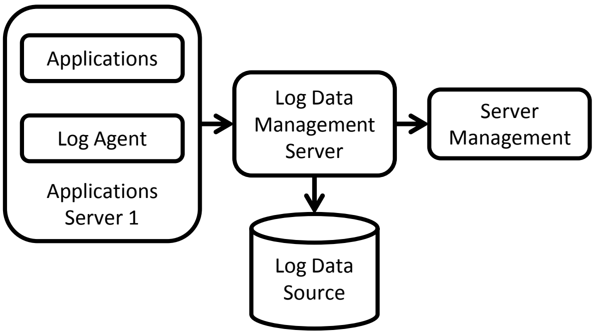


Figure 1. Use Case Diagram Description

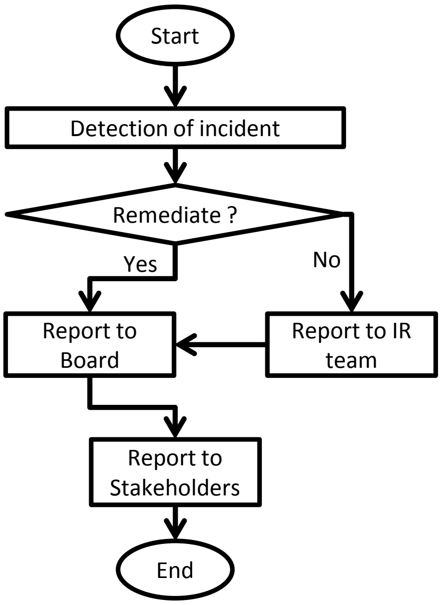


Figure 2. Data Flow Diagram

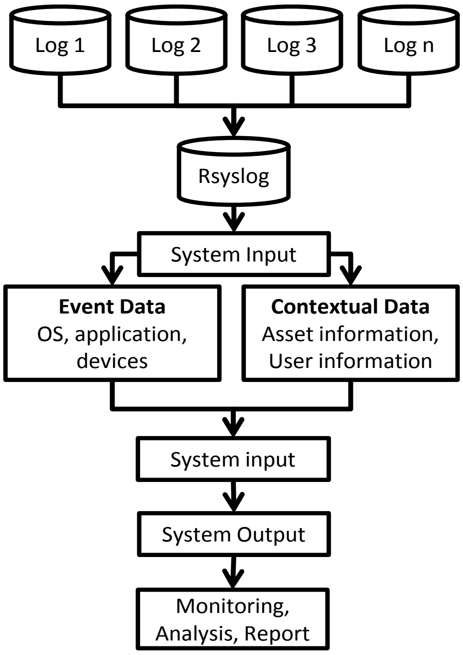


Figure 3. System Architecture Diagram

2.3 Security Requirements Measurements

1. Only limited number should have access to the admin functionality.
2. The password shall be more than 12 characters.
3. The password shall be changed every six months.
4. The SIEM system shall have a dedicated server and will not have any other application installed.

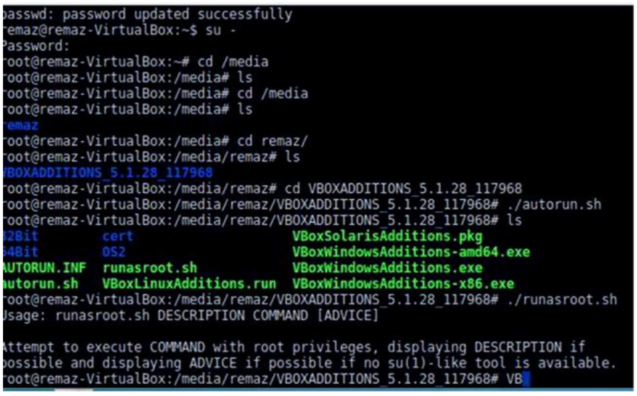
3. Result and discussion

VirtualBox is cross-platform virtualization software that enables users to stretch out their current computer to run different operating systems at the same time. Two machines Linux are created, one for SYSLOG server and another one for client. Besides that, one window server prepares to collect the logs form.

The sudo command will run that with high privileges. Elevated privileges are required to perform certain administrative tasks such as shut down or restart the computer. It is typically located at /etc/sudoers. The best and most secure way to alter this file is by utilizing the visudo command. This command will begin the vi editorial manager with elevated privileges so user can edit the document and save it. It additionally will put a filelock on the sudoers file with the goal that nobody else can edit it. Once finished editing it, it will parse the file for simple mistakes. It is a substantially more secure method for editing the sudo file than simply using any old text editor [5].

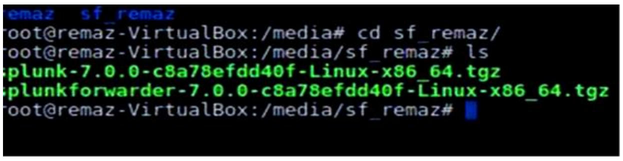
First, log in as a root by writing "su – "and put the password. Enter the directly by write "cd / name" to the directory. Write "ls" to see what is on the directly.(Figure 4)

After that, put splunk files in the share folder, then enter into it by "cd sf_remaz/" (Figure 5)



```
asswd: password updated successfully
emaz@remaz-VirtualBox:~$ su -
assword:
oot@remaz-VirtualBox:~# cd /media
oot@remaz-VirtualBox:/media# ls
oot@remaz-VirtualBox:/media# cd /media
oot@remaz-VirtualBox:/media# ls
emaz
oot@remaz-VirtualBox:/media# cd remaz/
oot@remaz-VirtualBox:/media/remaz# ls
BOXADDITIONS_5.1.28_117968
oot@remaz-VirtualBox:/media/remaz# cd VBOXADDITIONS_5.1.28_117968
oot@remaz-VirtualBox:/media/remaz/VBOXADDITIONS_5.1.28_117968# ./autorun.sh
oot@remaz-VirtualBox:/media/remaz/VBOXADDITIONS_5.1.28_117968# ls
2Bit        cert                    VBoxSolarisAdditions.pkg
4Bit        OS2                     VBoxWindowsAdditions-amd64.exe
UTORUN.INF  runasroot.sh            VBoxWindowsAdditions.exe
utorun.sh   VBoxLinuxAdditions.run  VBoxWindowsAdditions-x86.exe
oot@remaz-VirtualBox:/media/remaz/VBOXADDITIONS_5.1.28_117968# ./runasroot.sh
sage: runasroot.sh DESCRIPTION COMMAND [ADVICE]

ttempt to execute COMMAND with root privileges, displaying DESCRIPTION if
ossible and displaying ADVICE if possible if no su(1)-like tool is available.
oot@remaz-VirtualBox:/media/remaz/VBOXADDITIONS_5.1.28_117968# VB
```

Figure 4. Access the directly with coding "su -, cd/ and Is"

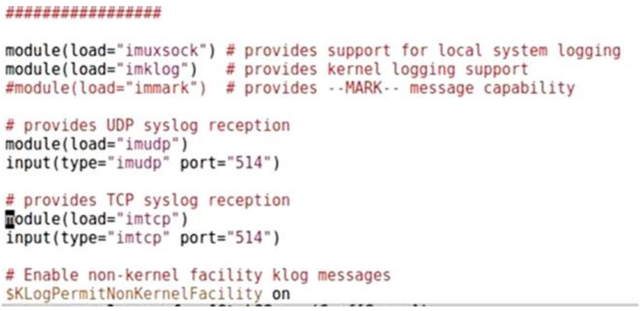


```
emaz   sf_remaz
oot@remaz-VirtualBox:/media# cd sf_remaz/
oot@remaz-VirtualBox:/media/sf_remaz# ls
plunk-7.0.0-c8a78efdd40f-Linux-x86_64.tgz
plunkforwarder-7.0.0-c8a78efdd40f-Linux-x86_64.tgz
oot@remaz-VirtualBox:/media/sf_remaz#
```

Figure 5. Locate the Splunk file for share folder

Copy the Splunk files to desktop for SYSLOG server. Then unzip the files in opt directly by writing "tar xvzf name file –C /opt". Enter to opt directly opt to start Splunk server by writing ". /splunk/bin/splunk start".Collect the log form client (dalal2) to SYSLOG. First bring up the SYSLOG server and login as root, and then check the IP address to change the local IP.

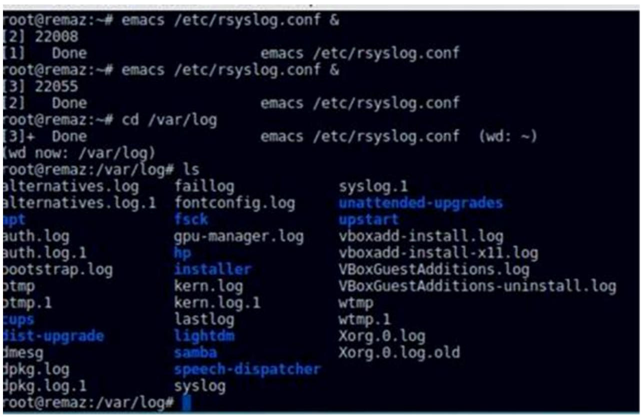
Install the Emacs (Figure 6). Pragmatically, it's extremely cool to see the utilize source code and have the ability to change it. This is particularly imperative for understudies and considerable measure of Emacs expansions is discernibly quicker on Linux [6].



```
##################

module(load="imuxsock") # provides support for local system logging
module(load="imklog")   # provides kernel logging support
#module(load="immark")  # provides --MARK-- message capability

# provides UDP syslog reception
module(load="imudp")
input(type="imudp" port="514")

# provides TCP syslog reception
module(load="imtcp")
input(type="imtcp" port="514")

# Enable non-kernel facility klog messages
$KLogPermitNonKernelFacility on
```

Figure 6. Emacs installation

See the SYSLOG in the same server by writing “cd /var/log” then “ls”.To see more, write more SYSLOG. (Figure 7)

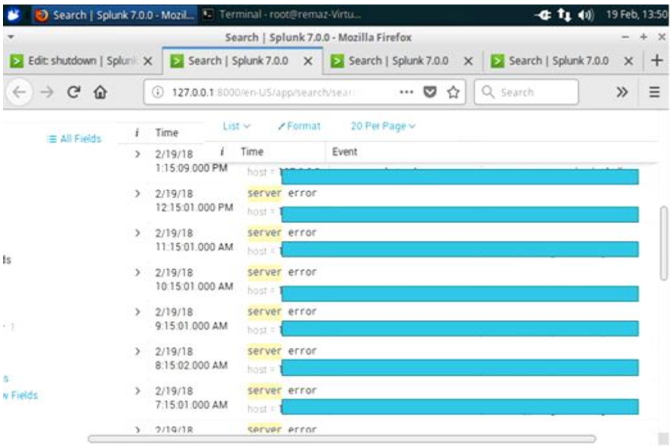


```
root@remaz:~# emacs /etc/rsyslog.conf &
[2] 22008
[1]   Done                    emacs /etc/rsyslog.conf
root@remaz:~# emacs /etc/rsyslog.conf &
[3] 22055
[2]   Done                    emacs /etc/rsyslog.conf
root@remaz:~# cd /var/log
[3]+  Done                    emacs /etc/rsyslog.conf  (wd: ~)
(wd now: /var/log)
root@remaz:/var/log# ls
alternatives.log    faillog            syslog.1
alternatives.log.1  fontconfig.log     unattended-upgrades
apt                 fsck               upstart
auth.log            gpu-manager.log    vboxadd-install.log
auth.log.1          hp                 vboxadd-install-x11.log
bootstrap.log       installer          VBoxGuestAdditions.log
btmp                kern.log           VBoxGuestAdditions-uninstall.log
btmp.1              kern.log.1         wtmp
cups                lastlog            wtmp.1
dist-upgrade        lightdm            Xorg.0.log
dmesg               samba              Xorg.0.log.old
dpkg.log            speech-dispatcher
dpkg.log.1          syslog
root@remaz:/var/log#
```

Figure 7. See SYSLOG from same server

Now, bring up the other machine (client) and etc the emacs (put the IP for SYSLOG server) to send all logs to SYSLOG server (Figure 8). All logs were sent to SYSLOG server and the logs can see in real time by writing tail –f syslog. By using Rsyslog Agent, writing the IP of syslog machine. The logs receive from JCH server.

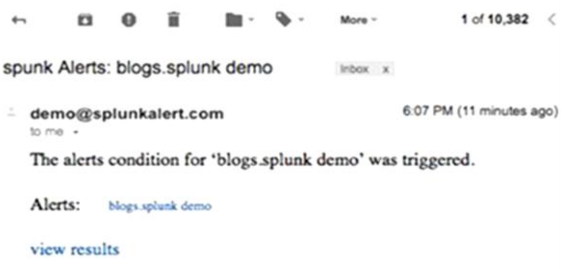
The e-mail configure alerts is demonstrated in Figure 9 as the blog splunk demo was triggered, the user may receive the email instantaneously.



Search | Splunk 7.0.0 - Mozil...
Terminal - root@remaz-Virtu...
19 Feb, 13:50
Search | Splunk 7.0.0 - Mozilla Firefox
Edit: shutdown | Splunk
Search | Splunk 7.0.0
Search | Splunk 7.0.0
Search | Splunk 7.0.0
127.0.0.1:8000/en-US/app/search/sear
Search
All Fields
List
Format
20 Per Page

i	Time	Event
›	2/19/18 1:15:09.000 PM	host = [redacted]
›	2/19/18 12:15:01.000 PM	server error host = [redacted]
›	2/19/18 11:15:01.000 AM	server error host = [redacted]
›	2/19/18 10:15:01.000 AM	server error host = [redacted]
›	2/19/18 9:15:01.000 AM	server error host = [redacted]
›	2/19/18 8:15:02.000 AM	server error host = [redacted]
›	2/19/18 7:15:01.000 AM	server error host = [redacted]
›	2/19/18	server error

Figure 8. Sending all file to SYSLOG server



spunk Alerts: blogs.splunk demo

demo@splunkalert.com
to me
6:07 PM (11 minutes ago)

The alerts condition for ‘blogs.splunk demo’ was triggered.

Alerts: blogs.splunk demo

view results

Figure 9. The e-mail configure alerts

4. Conclusion

This study successfully demonstrated the culling various source information under one platform for both preventive and detective controls as well as email alert. The system is designed to monitor all devices and networks through execution Splunk.

5. References

[1] Kavanagh K. M., Rochford O. and Bussa T. 2016. Magic quadrant for security information and event management, Gartner.

[2] Aguirre, I. and Alonso, S. 2012. Improving the automation of security information management: A collaborative approach. IEEE Security & Privacy. 10, 1, 55–59.

[3] Van Der Aalst, W. M. 2013. Business process management: a comprehensive survey. ISRN Software Engineering. 1-37.

[4] Di Sarno, C., Garofalo, A., Matteucci, I. and Vallini, M. 2016. A novel security information and event management system for enhancing cyber security in a hydroelectric dam. International

Journal of Critical Infrastructure Protection. 13, 39–51.

[5] Cannon, J. 2016. Linux Administration: The Linux Operating System and Command Line Guide for Linux Administrators.

[6] Stallman, R. M. 2007. Gnu Emacs Manual: For Version 22. Free Software Foundation.