SOC Syslog Playbook 2022

Further description of topics covered

Type of Systems: FreeBSD
Necessary Skills: FreeBSD admin (comparable but not the same as Linux),
Complete Goal:
Steps:

1) Check version

Relevant Info:

Appendix:

syslog.conf - This is the syslog configuration file

If syslog is not enabled on default , the variable “syslogd_enable” in /etc/rc.conf enables it.

Logstash plugin for syslog –

FreeBSD documentation isnt the most helpful when trying to configure logstash to syslogd

—---

From Wazuh documentation:

Rsyslog on Linux (THIS IS NOT FREEBSD)

Use rsyslog on a Linux host with a Wazuh agent to log to a file and send those logs to the environment.

Configure rsyslog to receive syslog events and enable the TCP or UDP settings by editing /etc/rsyslog.conf.

For TCP:

```
$ModLoad imtcp
$InputTCPServerRun <PORT>
```

For UDP:

```
$ModLoad imudp
$UDPServerRun <PORT>
```

Make sure to review your firewall/SELinux configuration to allow this communication.

Configure rsyslog to forward events to a file by editing /etc/rsyslog.conf.

```
# Storing Messages from a Remote System into a specific File
if $fromhost-ip startswith 'xxx.xxx.xxx.' then /var/log/<file_name.log>
& ~
```

To perform the following steps, make sure to replace <file_name.log> with the name chosen for this log.

Deploy a Wazuh agent on the same host that has rsyslog.

Configure the agent to read the syslog output file by editing /var/ossec/etc/ossec.conf.

```
<localfile>
<log_format>syslog</log_format>
<location>/var/log/<file_name.log></location>
</localfile>
```

Restart rsyslog and the Wazuh agent.

```
systemctl restart rsyslog
systemctl restart wazuh-agent
```

—---

They’re [logs] usually stored locally, but they can also be streamed to a central server if the administrator wants to be able to access all logs from a single location. By default, port 514 and UDP are used for the transmission of Syslogs.

configure Logstash listening on the TCP port first

We will forward our syslogs to TCP port 10514 of the virtual machine. Logstash will listen to port 10514 and collect all messages.

Let’s edit the configuration file of the syslog daemon.

```
sudo nano /etc/rsyslog.d/50-default.conf
```

Copy

Above the line “#First some standard log files. Log by facility” we’ll add the following:

```
*.*                         @@127.0.0.1:10514
```

To save the config file, we press CTRL+X, after which we type Y and finally press ENTER.

Restart Syslog Daemon

```
sudo systemctl restart rsyslog.service
```

If you don’t have a git tool available on your test system, you can install it with:

```
sudo apt update && sudo apt install git
```

```
sudo git clone
https://github.com/coralogix-resources/logstash-syslog.git
/etc/logstash/conf.d/logstash-syslog
```

https://syslog-ng.gitbooks.io/getting-started/content/chapters/chapter_0/section_4.html - seems pretty good