IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

Syslog Missing Identification And Handling Automation

[1] Mrunali Waykos, [2] Dr. Sachin Sakhare

[1]Post Graduate Student, [2]Associate Professor

[1] Department of Computer Engineering, [2] Department of Computer Engineering,

[1]Vishwakarma Institute of Information Technology, Pune, India

Abstract: Project is largely supported fault management under the service Assurance. Tata communication are using Monolith NMS tool for monitoring the Network Devices. All the Network Devices are available with vendors like Cisco, Juniper, Alcatel, and Huawei. All the information corresponding data maintaining by Cramer Whenever new device configured or terminated from the Network. Supposed any fault occurred on protocol level that point device will generate log and send to Monolith Collection server. Will Processing the logs supported multiple regular expression and process the Alarm. Monolith is integrated with Service Now for Ticketing and capable to book Proactive Ticket for the processed Alarm.

Index Terms **– Perl, UNIX Basics, SQL, PE Syslog Patterns.**

I. INTRODUCTION

Syslog may be a standard for sending and receiving notification messages–in a specific format–from various network devices. The messages include time stamps, event messages, severity, host IP addresses, diagnostics and more. All the information corresponding data maintaining by Cramer Whenever new device configured or terminated from the Network. Supposed any fault occurred on protocol level that point device will generate log and send to Monolith Collection server. Will Processing the logs supported multiple regular expression and process the Alarm. Monolith is integrated with Service Now for Ticketing and capable to book Proactive Ticket for the processed Alarm. Moreover, Syslog is open-ended. Syslog was designed to observe network devices and systems to channelize notification messages if there are any issues with functioning–it also sends out alerts for pre-notified events and monitors suspicious activity via the change log/event log of participating network devices. Logs aren't any longer limited to servers; they cover all networked systems including user terminals. Forensics related usage requires reliability and integrity [1]. In today's distributed heterogeneous environment, to confirm safe collection and archiving, dedicated resources are generally assigned for logging. Applications and devices will send the log messages to those collectors. Standard logging protocols are required for interoperability. Security mechanisms should be available to confirm the privacy, authenticity, and integrity of the messages. Over and above, log messages should be collected, reliably and without interruption [2].

II. PROBLEM DEFINITION

We need to spot Network Syslog's those are missing and notify to operation and IPNOC team. Different devices used for networking is definitely handled by syslog. Availability of enormous data makes the task of handling it even harder and predicting risks has never been easy. Device monitoring can't be possible one by one. So for avoiding those difficulties syslog is generated for each device.

III. SYSTEM ARCHITECTURE

Syslog may be a way for network devices to send event messages to a logging server – usually referred to as a Syslog server. The Syslog protocol is supported by a large range of devices and might be wont to log differing kinds of events [3]. as an example, a router might send messages about users logging on to console sessions, while a web- server might log access-denied events.

Most network equipment, like routers and switches, can send Syslog messages. Not only that, but nix servers even have the flexibility to get Syslog data, as do most firewalls, some printers, and even web-servers like Apache. Windows-based servers don't support Syslog natively, but an outsized number of third-party tools make it easy to gather Windows Event Log or IIS data and forward it to a Syslog server.

Unlike SNMP, Syslog can't be wont to "poll" devices to assemble information. As an example, SNMP encompasses a complex data structure that permits a management station to ask a tool for information on things like temperature data or available space. That's unfeasible with Syslog – it simply sends messages to a central location when specific events are triggered.

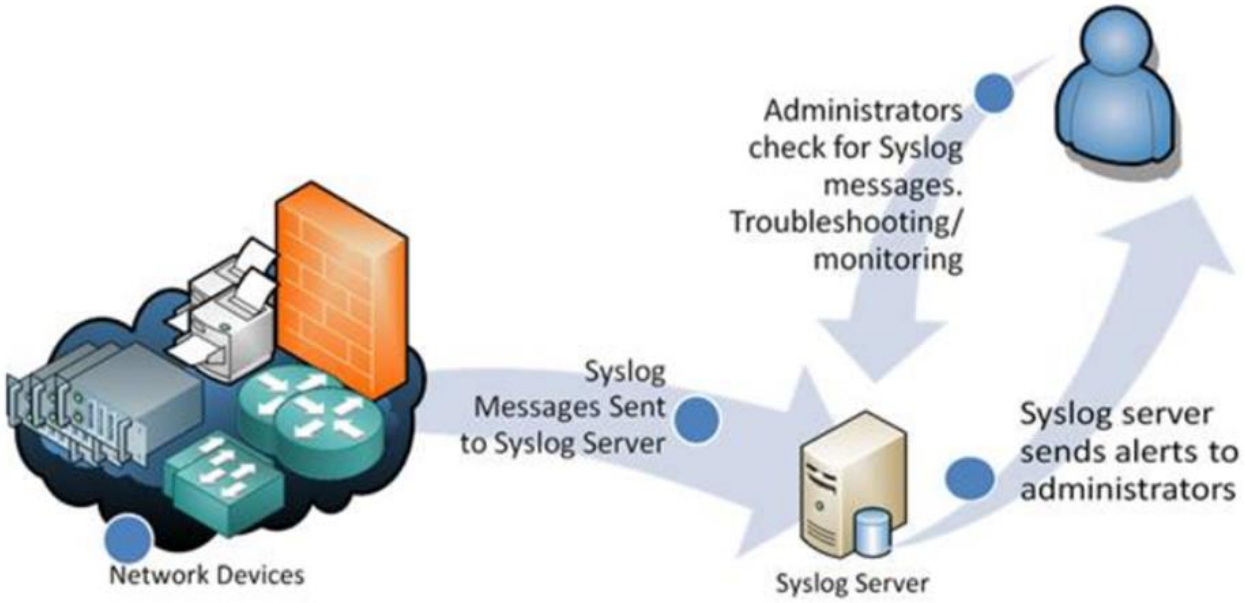

Fig. 1 System Architecture

IV. EXISTING SYSTEM

The below fig. is existing system of project. Where missing syslog is identify on syslog server. Then we have to take troubleshoot from NOC team by checking their IP address. And notify the missing syslog to customer by using Perl scripting.

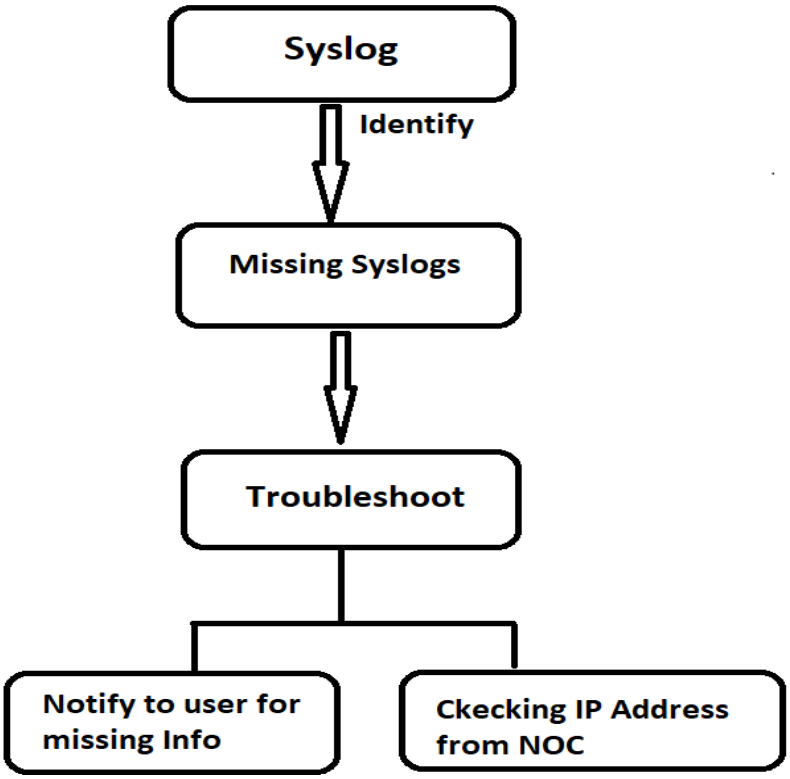

Fig. 2 Existing System

4.1 Missing Syslog Identification:

Syslog could be a format of string which is generated on every device. That device is generating one mail and stored in log file. Any style of fault occurred on any device than it'll generate the logs. Device is capable to send the log to any monitoring system on SNMP port 514 as default. All the device has configured by monolith collection layer IP where receiving syslog. We must check which syslog is missing and make their report by scripting. Identified the desired syslog that user can highlight the difficulty which devices faces. If syslog is missed, then read a computer file supported IP then convert it into CSV file. And lastly notify to customer by sending mail by Perl scripting.

4.2 Troubleshoot:

For troubleshooting, there's separate team called as NOC. If NOC team doesn't give us troubleshoot of any device then we must sign up Note dump. If IP not in note dump that's receiving from NOC device details which means device is dead. Then Notify to customer for missing information by Perl scripting.

4.3 Managing Syslog:

SNMP could be a standard protocol for monitoring and managing systems within the Internet. A logging system should be seamlessly manageable using SNMP. For that purpose, managed objects have to be defined as Management Information Base.

4.4 Working:

We must do Perl coding for reading the CSV file for file handling and browse log file and convert it into zip file. Then compare the IP list within the CSV file and notify to customer by Perl scripting. And also, frequently monitor the missing syslogs and provides update to customer manually through cronjob scheduler for whole day. The below is the working flow of project:

a. Perl code -CSV file read
   |
   File handling

b. Perl code – Read log file – convert into ZIP file
   |
   Notify to customer

c. Perl code – Manually create cronjob scheduler for whole day

4.5 Cronjob Scheduler:

Cronjob scheduler is that the task scheduler, where task is scheduled by date and time. This is often a straightforward thanks to remember what that task does. To run a “Cron Job” task that runs quite once every day, Click Daily task. Recur daily and repeat the task every (How often you would like the task to run. you'll be able to type in other options during this field than what's given) and take care to click enabled. At the moment click Okay and click on the tab “Actions” and New.

V. IMPLEMENTATION OF SYSLOG

5.1 Syslog Backend Details:

In this fig: Syslog backend details shows the details of the customer where the syslog came in a particulate pattern.it indicates the date of the event , timing of the event, VPRN no, BGP warnings, router configuration, and IP address.

custom2	IPAddress
<188>Apr 23 00:00:09 192.168.235.103 TMNX: 2891563 vprn101447 BGP-WARNING-bgpRemoteEndClosedConn-2011 [Peer 266: 10.100.101.238]:	192.168.235.103
<188>Apr 23 00:00:12 192.168.235.98 TMNX: 2487325 vprn506558 BGP-WARNING-bgpRemoteEndClosedConn-2011 [Peer 1731: 10.215.70.54]:	192.168.235.98
<188>Apr 23 00:00:26 192.168.201.2 TMNX: 4050703 vprn115721 BGP-WARNING-bgpBackwardTransition-2002 [Peer 50: 10.241.2.46]: VR 5(	192.168.201.2
<188>Apr 23 00:00:27 192.168.194.92 TMNX: 4456345 vprn500281 BGP-WARNING-bgpBackwardTransition-2002 [Peer 437: 10.125.161.153]:	192.168.194.92
<188>Apr 23 00:00:33 192.168.194.11 TMNX: 2566905 vprn6891 BGP-WARNING-bgpBackwardTransition-2002 [Peer 129: 10.125.160.45]: VR	192.168.194.11
<188>Apr 23 00:00:37 192.168.240.129 TMNX: 4225236 vprn500111 BGP-WARNING-bgpBackwardTransition-2002 [Peer 861: 172.23.28.226]:	192.168.240.129
<188>Apr 23 00:00:44 192.168.192.163 TMNX: 1650992 vprn120312 BGP-WARNING-bgpBackwardTransition-2002 [Peer 1806: 10.25.148.106]:	192.168.192.163
<188>Apr 23 00:00:48 192.168.194.77 TMNX: 13499964 vprn110581 BGP-WARNING-bgpBackwardTransition-2002 [Peer 43: 10.77.11.50]: VR	192.168.194.77
<188>Apr 23 00:01:19 192.168.194.92 TMNX: 4456362 vprn112393 BGP-WARNING-bgpBackwardTransition-2002 [Peer 249: 10.95.97.70]: VR	192.168.194.92
<188>Apr 23 00:01:19 192.168.235.98 TMNX: 2487363 vprn506558 BGP-WARNING-bgpRemoteEndClosedConn-2011 [Peer 1731: 10.215.70.154]:	192.168.235.98
<188>Apr 23 00:00:39 192.168.228.110 TMNX: 16558905 vprn1295 BGP-WARNING-bgpBackwardTransition-2002 [Peer 87: 10.210.141.166]: \	192.168.228.110
<188>Apr 23 00:02:05 192.168.235.103 TMNX: 2891582 vprn1860 BGP-WARNING-bgpRemoteEndClosedConn-2011 [Peer 77: 10.75.70.34]: VR '	192.168.235.103

Fig. 3 Syslog Backend

5.2 Syslog Alarm INFO:

In the fig: Syslog Alarm represents the device the AlarmId, AlarmKey, Name of device where the location of the device and name of the device is. The events will be converted into alarms. That alarms can be process for making the ticket in service now for resolving the device problem.

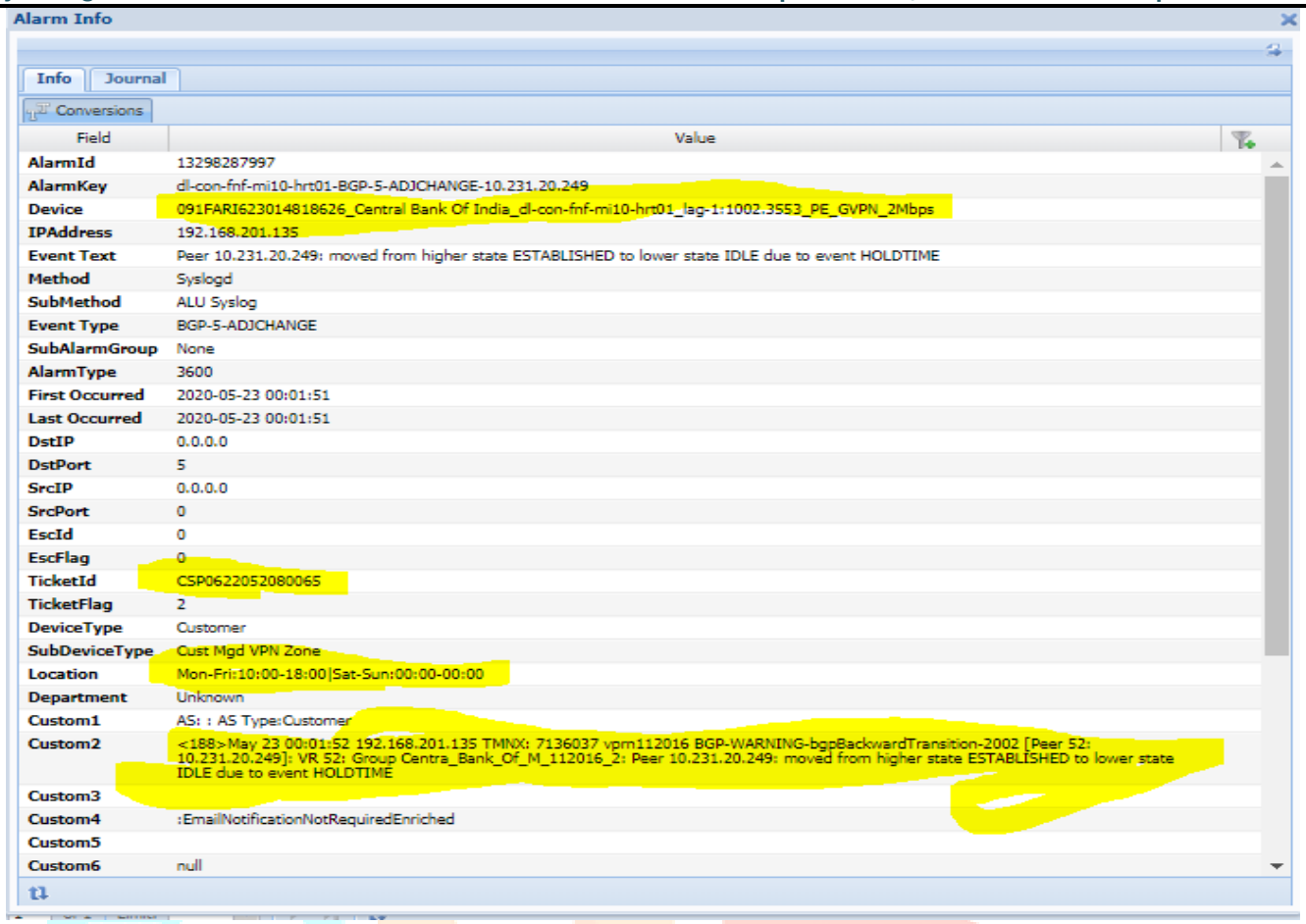

Fig. 4 Syslog Alarm

5.3 Monolith UI for Alarm INFO:

The below fig: Monolith UI Alarm shows the problem of any device on port 510 where the syslog is missing. That syslog can generate event and will be processed foe alarms. In Monolith UI, it indicates the device alarm info, device name, device type, event type, event text, count of event, last event occurred, and the customer details.

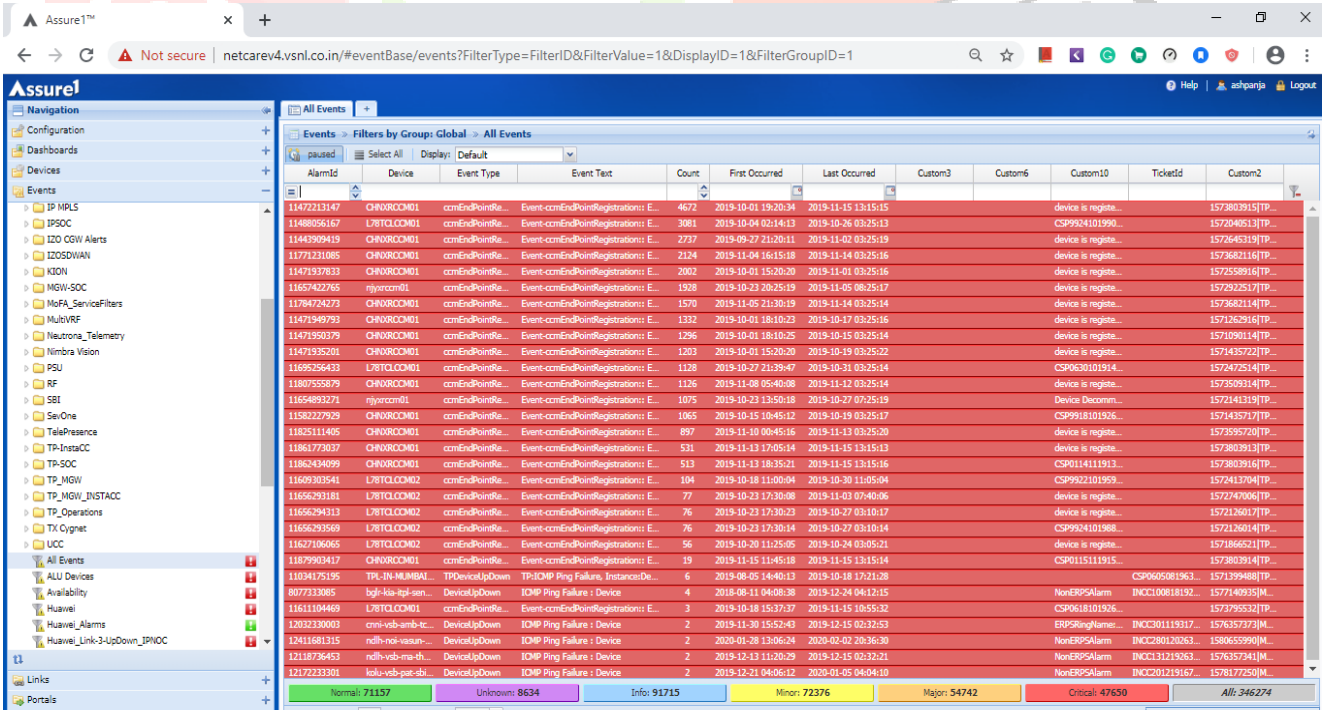

Fig. 5 Monolith UI for Alarm

5.4 Backend Processing Syslog:

The below fig: Backend processing syslog shows that the exact problem of the device. That device can generate the massage in a format and send to the NOC team. That team will process the issue for in log file. That log file we have to operate using Perl scripting to identify in which device syslog is missing.

Log (EventSyslogMPLS_NOC.log)

Timestamp	Log Level	TID	Message
2020-05-23 21:01:53	DEBUG	8	Ran Base Rules
2020-05-23 21:01:53	DEBUG	9	Base Rules:SyslogKey[Down~detected egress FCS errors Down~ICC:UNUSUAL_ERROR Down~PCI ERROR Down~CHASSISD_FRU_OFFLINE_NOTICE Down~CHASSISD_IPC_CONNECTION_DROPPED Down~WI CPQ LastUpdateTime Down~Failed ICC transaction Down~Major Errors - XM Chip Down~PWRFAILURE Down~ESWD_LEARNT_FDB_MEMORY_ERROR Down~TOXIC_SFP Down~WEDGE DETECTED Down~PCI Fatal Error Down~CHASSISD_IFDEV_DETACH_FPC Down~IXCHIP Down~parity error detected in mpfe0 Down~NAND-MEDIACK Down~PLL Error Down~MALLOCFAIL Down~IX PCI: PIO Down~PWRCYCLE Down~PLL Error code]
2020-05-23 21:01:53	DEBUG		... Aggregator Active, processing event #1199965
2020-05-23 21:01:53	DEBUG	5	Base Rules:Before Key Match[Down][ESWD_LEARNT_FDB_MEMORY_ERROR]
2020-05-23 21:01:53	ALWAYS	3	##################################
2020-05-23 21:01:53	ALWAYS	3	Base Rules -> IPAddress 192.168.208.66 and node is [192.168.208.66]
2020-05-23 21:01:53	DEBUG	2	Base Rules:SyslogKey[Down~detected egress FCS errors Down~ICC:UNUSUAL_ERROR Down~PCI ERROR Down~CHASSISD_FRU_OFFLINE_NOTICE Down~CHASSISD_IPC_CONNECTION_DROPPED Down~WI CPQ LastUpdateTime Down~Failed ICC transaction Down~Major Errors - XM Chip Down~PWRFAILURE Down~ESWD_LEARNT_FDB_MEMORY_ERROR Down~TOXIC_SFP Down~WEDGE DETECTED Down~PCI Fatal Error Down~CHASSISD_IFDEV_DETACH_FPC Down~IXCHIP Down~parity error detected in mpfe0 Down~NAND-MEDIACK Down~PLL Error Down~MALLOCFAIL Down~IX PCI: PIO Down~PWRCYCLE Down~PLL Error code]
2020-05-23 21:01:53	DEBUG	1	Syslog => [<7>May 23 20:59:38 coi-t2-icr02 kernel: rts_commit_proposalmput op: 2, peer_type:17, peer_index:0, vskid:0, seqno:515660631, flag:9,]
2020-05-23 21:01:53	DEBUG	12	====> Inserting Field [Count] Value [1]
2020-05-23 21:01:53	DEBUG	7	Base Rules:Before Key Match[Down][NAND-MEDIACK]
2020-05-23 21:01:53	DEBUG	8	Log 1:Print Node [[192.168.203.195]] and IP [192.168.203.195]
2020-05-23 21:01:53	DEBUG	10	Base Rules:Before Key Match[Down][PWRCYCLE]
2020-05-23 21:01:53	DEBUG	5	Base Rules:Before Key Match[Down][TOXIC_SFP]
2020-05-23 21:01:53	DEBUG	9	Base Rules:Before Key Match[Down][detected egress FCS errors]
2020-05-23 21:01:53	INFO		RxDevice License # 1095
2020-05-23 21:01:53	ALWAYS	3	Base Rules -> Database connection is succesful
2020-05-23 21:01:53	DEBUG	6	Message Received: <7>May 23 20:59:38 coi-t2-icr02 kernel: rts_commit_proposalmput op: 2, peer_type:17, peer_index:1, vskid:0, seqno:515660631, flag:9,
2020-05-23 21:01:53	ALWAYS	1	##################################
2020-05-23 21:01:53	DEBUG	7	Base Rules:Before Key Match[Down][PLL Error]
2020-05-23 21:01:53	DEBUG	10	Base Rules:Before Key Match[Down][PLL Error code]
2020-05-23 21:01:53	DEBUG	2	Base Rules:Before Key Match[Down][detected egress FCS errors]
2020-05-23 21:01:53	DEBUG	5	Base Rules:Before Key Match[Down][WEDGE DETECTED]
2020-05-23 21:01:53	ALWAYS	1	Base Rules -> Started
2020-05-23 21:01:53	DEBUG	8	Message Received: <3>May 23 20:59:38 cn-me01-icr03 kernel: mld6_input: src :: is not link-local (grp=ff02::2)

Fig. 6 Backend Processing Syslog

VI. HANDLING AUTOMATION

6.1 Customer to notify:

Using Perl scripting we have to notify to customer by sending mail where exact issues occurred in the device.

6.2 Make Scheduler:

Task scheduler is one of the most practical applications because it can streamline your work. The main purpose of the task scheduler is to trigger the running of different scripts and programs at a specific time or a certain event. It has a library where all the task loaded are indexed and it organizes them according to the time that must be done and their importance.

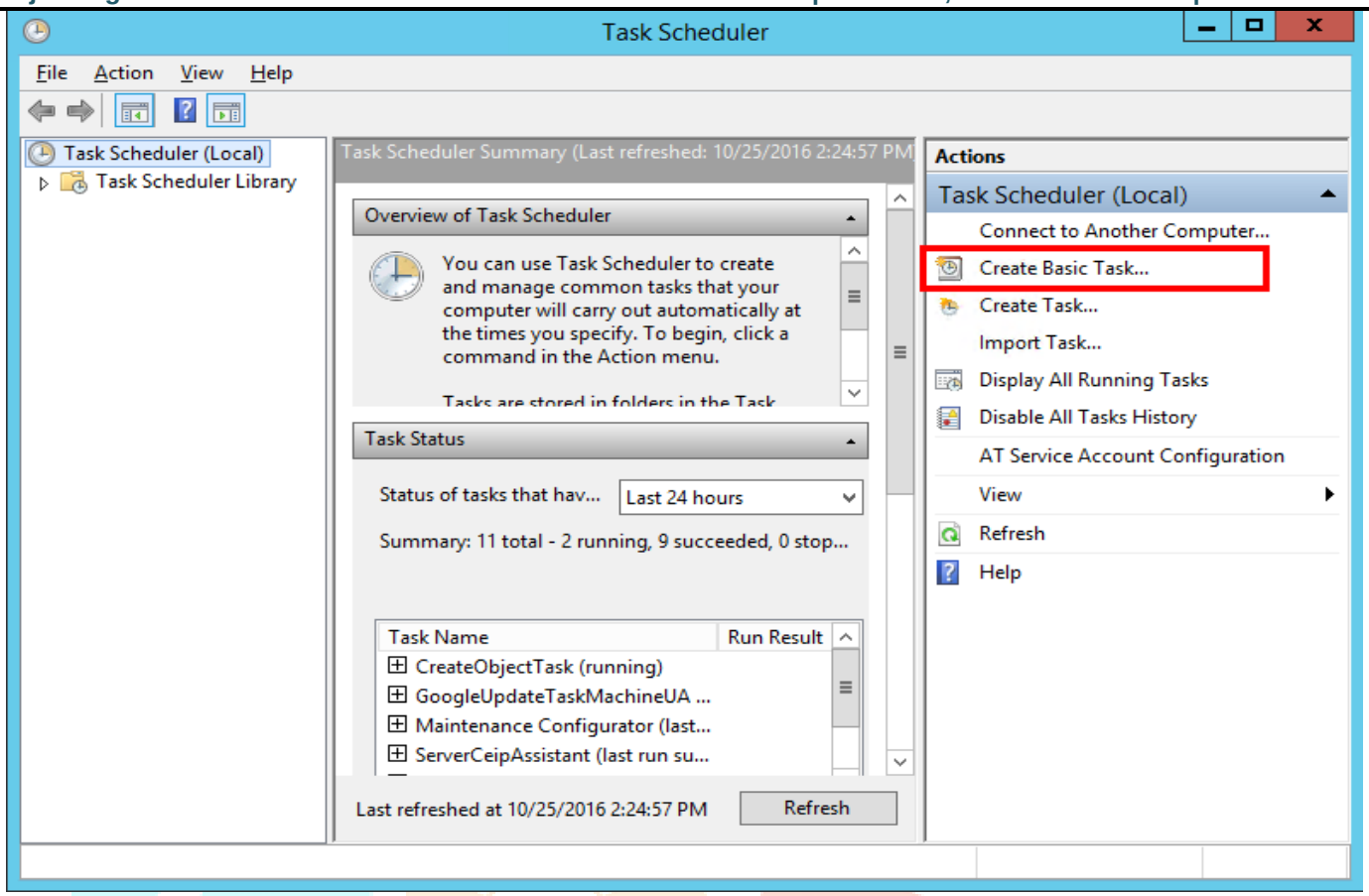

Fig. 7 Task Scheduler

VII. Result

Conclude that, Identified the syslog gaps proactively and May fulfilled the gaps and provides time to time updating to customer by sending mail through Perl scripting. And identify the missing syslog using previous data. And generate alarms for creating their ticket by third team for further process. Using Syslog, it's very helpful for company to convey better services to customer. I've got used a SNMP protocol for assess any failure points quickly. The appliance monitors configuration information of syslog applications in an exceedingly network, analyzes monitored configuration and visualizes the results on report.

VIII. Acknowledgment

I would prefer to take this chance to increase my gratitude to Vishwakarma Institute of knowledge Technology, Pune, under Savitribai Phule Pune University for providing the platform for my work.

References

[1] B. Bock, D. Huemer, and A Min Tjoa. Towards More Trustable Log Files for Digital Forensics by Means of Trusted Computing. In Advanced Information Networking and Applications (AINA), 2010 24th IEEE International Conference on, pages 1020–1027, April 2010.

[2] J. Salowey, T. Petch, R. Gerhards, and H. Feng. Datagram Transport Layer Security (DTLS) Transport Mapping for Syslog. RFC6012, October 2010.

[3] F. Miao, Y. Ma, and J. Salowey. Transport Layer Security (TLS) Transport Mapping for Syslog. RFC5425, March 2009

[4] R. Gerhards. The Syslog Protocol. RFC5424, March 2009

[5] A. Okmianski. Transmission of Syslog Messages over UDP. RFC5426, March 2009.

[6] J. Kelsey, J. Callas, and A. Clemm. Signed Syslog Messages. RFC5848, May 2010.

[7] Syslog Agents on Windows [Online]. Available: http://sflanders.net/2013/10/25/syslog-agents-windows/

[8] Rsyslog [Online]. Available: http://www.rsyslog.com/

[9] Syslog-ng. [Online]. Available: http://www.balabit.com/network-security/syslog-ng/