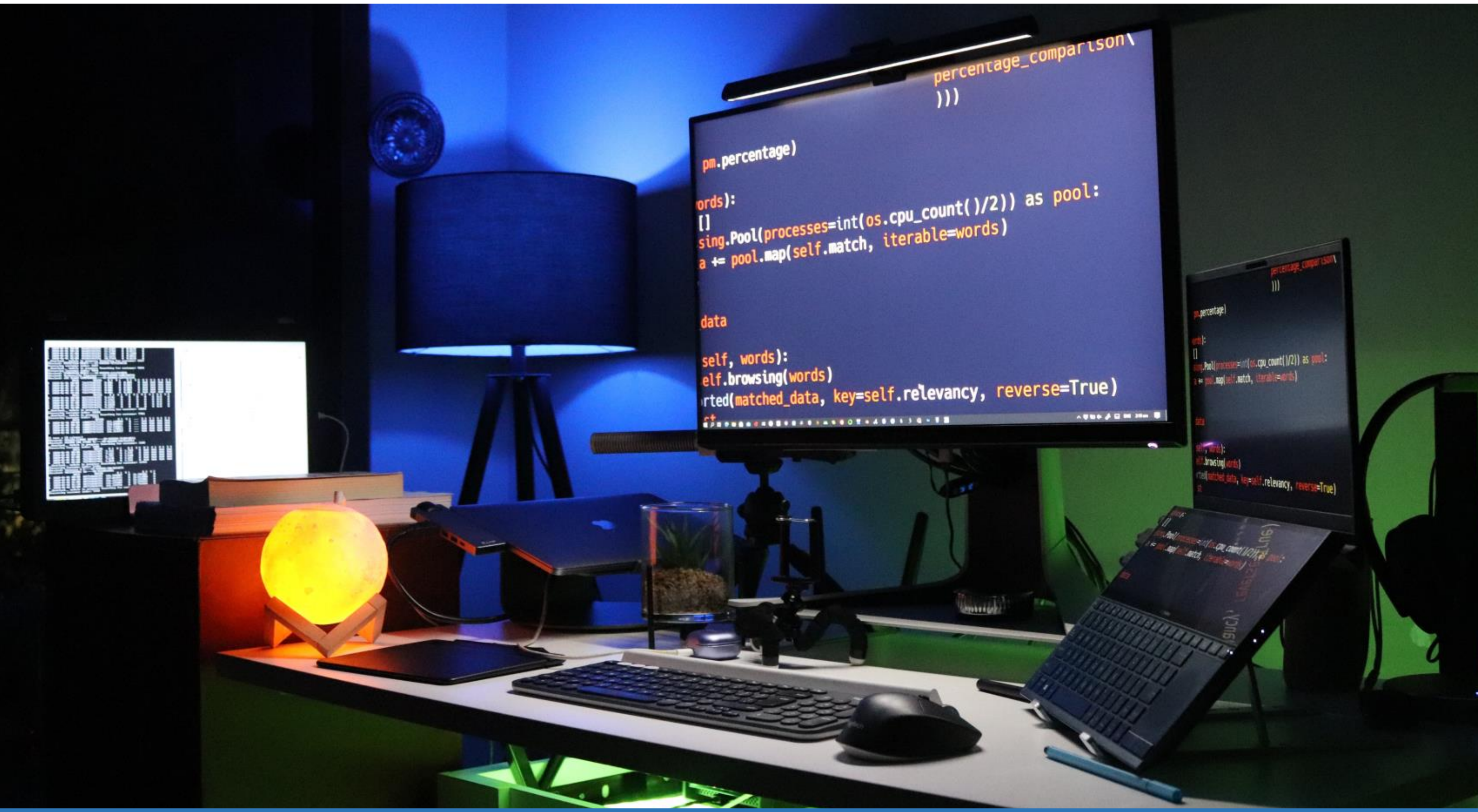
csstel


percentage_comparison\
)))
pm.percentage)
ords):
[]
sing.Pool(processes=int(os.cpu_count()/2)) as pool:
a += pool.map(self.match, iterable=words)
data
self, words):
elf.browsing(words)
rted(matched_data, key=self.relevancy, reverse=True)

AN-862103

Syslog Monitoring & Collection

Document No.: AN-862103, Rev 1.00
Applicable Products: ComView NX(S/M/L/X)
Contact: support@csstel.com
Web: www.csstel.com

Introduction

ComView offers a suite of network-based applications. One of which is Syslog Monitor app developed based on Syslog-NG, an open-source log management solution. Syslog Monitor lets users monitor syslog messages from syslog-capable network devices (i.e., syslog agents) for user-definable alarm conditions with automatic corrective actions and immediate alarm notifications. Optionally, Syslog Monitor can also log all messages from agents in an external USB drive for further processing and management.

Syslog Monitor app can be an ideal solution for users who manage servers and network devices to get real-time alerts on conditions that matter the most to their operations, while having the ability to archive all system logs for future deposition.

This application note is intended to provide an overview of Syslog Monitor app, how to configure it, and how to set up syslog agents to forward logs to ComView device for alarm monitoring and log collection.

This application note does not provide detailed description of how to use ComView, its connectivity and configuration, and other supporting information, as these are beyond the scope of this document. Refer to other resources for more details.

References:

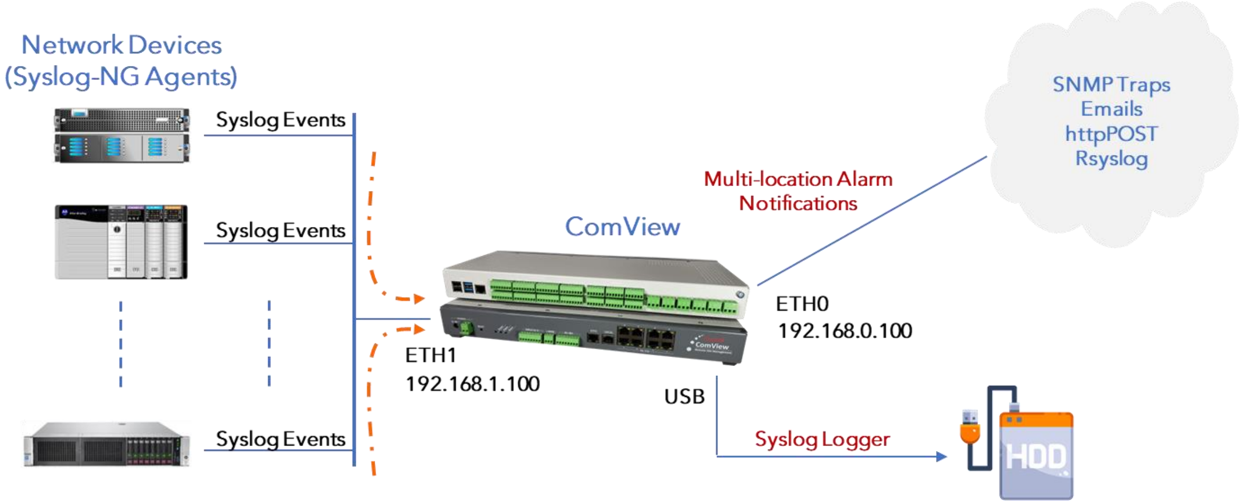
[1]. ComView - User Guide

[2]. Syslog-NG - https://www.syslog-ng.com/

[3]. Log rotate - https://manpages.ubuntu.com/manpages/xenial/man8/logrotate.8.html

Setup Overview

The diagram below illustrates the setup used in this application note.



From the above,

- Network devices are connected to ComView Ethernet 1 (ETH1, at IP address 192.168.1.100)
- Network devices must support Syslog-NG and be configured to send logs to ComView
- External USB drive is connected to ComView USB port and mounted as a media storage device to store logs

In this application note, our goal is to configure Syslog Monitor app to receive logs from network devices, to set up external USB drive to store logs, to configure network devices to send logs, and to define alarm conditions for Syslog Monitor to detect alarms.

Syslog Monitor App

Syslog Monitor app is based on Syslog-NG which takes logs from different sources and forwards them to various destinations.

Syslog Monitor uses three configuration files:

- '/usr/cvconf/syslog-ng.conf.dis'
- '/usr/cvconf/syslog-ng.conf.en'
- '/usr/cvconf/cvLogs'

When no logging (i.e., no log collection) is required, Syslog Monitor loads 'syslog-ng.conf.dis' as the configuration file (i.e., 'syslog-ng.conf') for syslog-ng daemon. When logging is required, it loads 'syslog-ng.conf.en' instead.

syslog-ng.conf.dis

The following is the file default content that users may edit for their specific operational requirements:

```
@version: 3.27
@include "scl.conf"
@include "`scl-root`/system/tty10.conf"
options {
  time-reap(30);
  mark-freq(10);
  keep-hostname(yes);
  create_dirs(yes);
  dir-owner("root");
  dir-perm(0664);
};

source s_network { default-network-drivers(); };                         [1]

destination d_cvpipe { pipe("/tmp/cvnpipes/cvSyslogAppInt"); };          [2]

log { source(s_network); destination(d_cvpipe); };
```

Notes:

[1] Syslog Monitor uses 'default-network-drivers' to listen to log messages on ports:
- 514, both TCP and UDP, for RFC3164 (BSD-syslog) formatted traffic
- 601 TCP, for RFC5424 (IETF-syslog) formatted traffic
- 6514 TCP, for TLS-encrypted traffic

[2] This statement must remain unchanged as the application uses this named pipe for reading log messages

syslog-ng.conf.en

The following is the file default content that users may edit for their specific operational requirements:

```
@version: 3.27
@include "scl.conf"
@include "`scl-root`/system/tty10.conf"
options {
  time-reap(30);
  mark-freq(10);
  keep-hostname(yes);
  create_dirs(yes);
  dir-owner("root");
  dir-perm(0664);
};

source s_network { default-network-drivers(); };                     [1]

destination d_cvpipe { pipe("/tmp/cvnpipes/cvSyslogAppInt"); };       [1]
destination d_cvLogs {                                                [2]
  file(
    "/media/usb-drive/cvLogs_$HOST/cvSyslog"
    owner("root")
    group("root")
    perm(0664)
   );
};

log { source(s_network); destination(d_cvpipe); destination(d_cvlogs);}; [3]
```

Notes:

[1] As described previously

[2] An external USB drive is specified as the second destination. Log messages are logged in '/media/usb-drive' directory followed by the network device hostname sub-directory, and the log filename. Sub-directories are auto created, and files in each sub-directory are rotated according to '/usr/cvconf/cvLogs' file entries.

[3] Users must connect an external USB drive to one of the device USB ports and mount it as '/media/usb-drive', where '/media' is the system pre-defined directory and 'usb-drive', user-definable directory name. This directory name '/media/usb-drive' must be the same in '/usr/cvconf/cvLogs' file.

cvLogs

Syslog Monitor uses 'cvLogs' as configuration file and submits it to '/etc/logrotate.d' directory for logrotate utility to auto rotate 'cvSyslog' files in each subdirectory in the USB drive. The file has the following default content that users may edit for their specific operational requirements:

```
/media/usb-drive/cvLogs_*/cvSyslog
{
        rotate 60
        daily
        missingok
        create 0644 root root
        compress
        dateext
        dateformat -%Y%m%d
        postrotate
                invoke-rc.d syslog-ng reload > /dev/null
        endscript
}
```

Notes:

[1] Users can specify the number of file rotations and its frequency. In this setting, the file is rotated daily for 60 times with a filename in cvSyslog-YYYYMMDD format

[2] After rotation, logrotate restarts syslog-ng service

USB Drive Setup

When Syslog Monitor is configured to log syslog events from network devices, an external USB drive with sufficient capacity is needed for mass storage.

To add a USB drive to ComView, users must create a directory (e.g., 'usb-drive') on the drive to hold logs, mount the drive (e.g., '/media/usb-drive'), and set up auto mount on system bootup.

The following illustrates the general steps to be taken:

- Login ComView web interface and navigate to CONFIGURATION → NET APP/Syslog Monitor and set 'Syslog Data Logging Enable' to 'No'
- Soft restart or system reboot the device to disable data logging function to avoid logging data to the device internal flash storage
- Connect a pre-formatted USB drive (in NTFS or exFAT) to a USB port of ComView
- SSH to ComView and exit to shell environment to perform the following tasks using command lines:

```
$ sudo mkdir /media/usb-drive   ; create usb-drive directory in /media
```

```
$ sudo fdisk -l                 ; list all drives
Disk /dev/mmcblk0: 29.12 GiB, 31267487744 bytes, 61069312 sectors
Units: sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disklabel type: dos
Disk identifier: 0xab86aefd

Device         Boot  Start      End  Sectors  Size Id Type
/dev/mmcblk0p1 *      2048   526335   524288  256M  c W95 FAT32 (LBA)
/dev/mmcblk0p2      526336 61069278 60542943 28.9G 83 Linux


Disk /dev/sda: 29.3 GiB, 31457280000 bytes, 61440000 sectors
Disk model: SeaGlassUSB
Units: sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disklabel type: dos
Disk identifier: 0xf472032d

Device     Boot Start      End  Sectors  Size Id Type
/dev/sda1  *      128 61439999 61439872 29.3G  7 HPFS/NTFS/exFAT
```

Note: '/dev/sda1' is the name given by the OS to the attached USB drive

```
$ ls -l /dev/disk/by-uuid/*     ; list drives by UUID (Universally Unique ID)

lrwxrwxrwx 1 root root 15 Nov  2 02:44 /dev/disk/by-uuid/483efb12-d682-4daf-
9b34-6e2f774b56f7 -> ../../mmcblk0p2
lrwxrwxrwx 1 root root 15 Nov  2 02:43 /dev/disk/by-uuid/B726-57E2 ->
../../mmcblk0p1
lrwxrwxrwx 1 root root 10 Nov  2 02:52 /dev/disk/by-uuid/F422D4BE22D486D0 ->
../../sda1
```

Note: USB drive in this demo has UUID of F422D4BE22D486D0

```
$ sudo nano /etc/fstab          ; add the third line as below to auto mount
LABEL=writable  /        ext4   defaults        0 0
LABEL=system-boot       /boot/firmware  vfat    defaults        0       1
/dev/disk/by-uuid/F422D4BE22D486D0  /media/usb-drive auto 0 0
```

- Login ComView web page and set ‘Syslog Data Logging Enable’ to ‘Yes’ to enable logging after mounting the USB drive
- Soft restart or system reboot for changes to take effect
- SSH to ComView, exit to shell environment, and issue the following commands to list directories and files:

  ```
  $ sudo ls -l /media/usb-drive
  $ sudo ls -l /media/usb-drive/cvLogs_<hostname>
  ```

Notes:

- Commands to mount and unmount USB drive:

  ```
  $ sudo mount /media/usb-drive          ; mount
  $ sudo umount /media/usb-drive         ; unmount
  ```

- Unmount USB drive prior to detaching it from the device
- Repeat the steps in this section when a different USB drive is used

Syslog-NG Agent

To send syslog messages to ComView for collection and alarm monitoring, network devices must have support for syslog-ng. Configuring syslog-ng for these devices is operating system dependent.

The following is a sample syslog-ng configuration file for a Ubuntu-based network device. Users edit this file and install it in the network device as '/etc/syslog-ng/syslog-ng.conf':

```
#===============================================================================
# This syslog-ng configuration file is a TEMPLATE for DEBIAN syslogd compatible
# network devices that send syslog events to ComView, Syslog Monitor/receiver.
# For Ubuntu host, this file is to be installed at:
#   "/etc/syslog-ng/syslog-ng.conf"
#
# Users edit this file according to their logging needs
#===============================================================================

@version: 3.27
@include "scl.conf"
@include "`scl-root`/system/tty10.conf"

#===============================================================================
# Sources:
# - List of common log files
#===============================================================================
source s_local { system(); internal(); };
source s_auth { file("/var/log/auth.log"); };
source s_cron { file("/var/log/cron.log"); };
source s_daemon { file("/var/log/daemon.log"); };
source s_kern { file("/var/log/kern.log"); };
source s_mail { file("/var/log/mail.log"); };
source s_syslog { file("/var/log/syslog"); };
source s_user { file("/var/log/user.log"); };
source s_debug { file("/var/log/debug"); };
source s_error { file("/var/log/error"); };
source s_messages { file("/var/log/messages"); };

#===============================================================================
# Destinations:
# - List of log receivers defined by IP address and port number
#===============================================================================
destination d_logserver1 { syslog("192.168.1.100" transport("tcp") port(514));};

#===============================================================================
# Log paths:
# - Comment/remove the sources that do not require logging
#===============================================================================
log {
  source (s_local);
  source (s_auth);
  source (s_cron);
  source (s_daemon);
  source (s_kern);
  source (s_mail);
  source (s_syslog);
  source (s_user);
  source (s_debug);
  source (s_error);
  source (s_messages);
  destination (d_logserver1);
};
```

Alarm Configuration

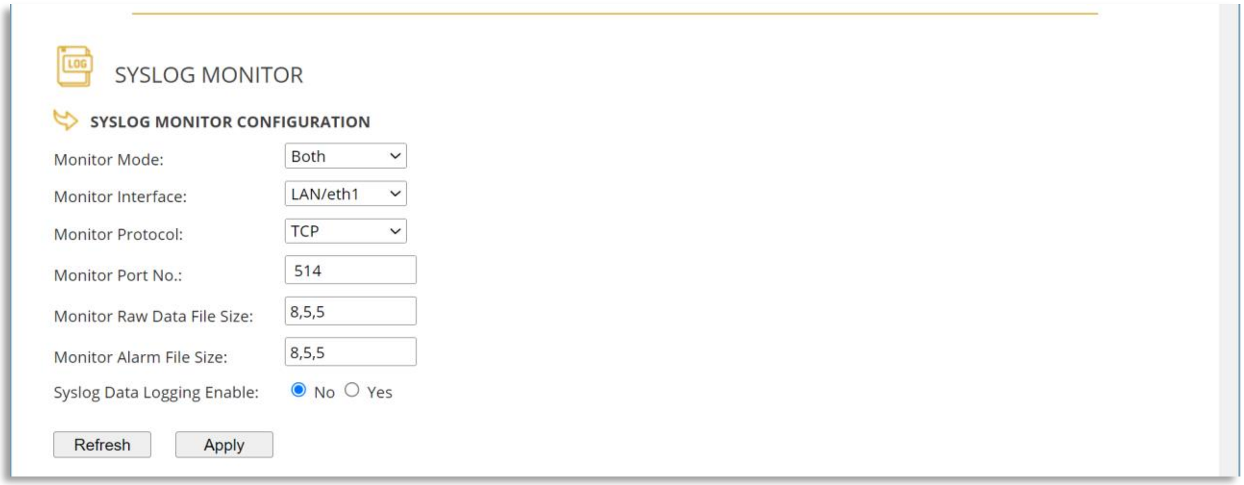
You can configure alarm conditions of Syslog Monitor app using one of the following:

- Online web interface
- Online editing of text-based device configuration file
- Uploading device configuration file

In this application note, we use web interface to define alarm condition 0, 1, and 2 to detect syslog messages that contain 'Invalid user', 'Failed password', and 'Accepted password' signatures to detect login events. In Ubuntu/Linux operating system, these signatures come from authentication log '/var/log/auth.log' for failed and successful login attempts. Once detected, we want to be notified by ComView in real-time so corrective action can be taken.

To do this, you log on ComView via its web interface and navigate to 'CONFIGURATION -> NET APP'. For ease of use, an app is configured on one web page only.

Syslog Monitor has two sections of configuration. The first section lets you select whether syslog collection is required by setting 'Syslog Data Logging Enable' radio input to 'Yes' or 'No', as shown in the screenshot below:



SYSLOG MONITOR

SYSLOG MONITOR CONFIGURATION

Monitor Mode: Both

Monitor Interface: LAN/eth1

Monitor Protocol: TCP

Monitor Port No.: 514

Monitor Raw Data File Size: 8,5,5

Monitor Alarm File Size: 8,5,5

Syslog Data Logging Enable: ● No ○ Yes

Monitor Mode:

Description: To define operating mode of Syslog Monitor

Usage: Select from dropdown list [Raw, Alarm, Both, None]:

- Raw: Data collection mode, data received is logged in raw data file
- Alarm: Alarm monitoring mode, lines of data that meet alarm conditions are logged in common alarm file
- Both: Data collection and Alarm monitoring mode
- None: No data collection and alarm monitoring, however, logging is still active if Syslog Data Logging Enable is set to Yes

Monitor Interface:

Description: To define the Ethernet interface of Syslog Monitor

Usage: Select from dropdown list [WAN/eth0, LAN/eth1]

Monitor Protocol:

Description: To define network protocol of Syslog Monitor

Usage: Select from dropdown list [TCP/UDP]

Monitor Port No.:

Description: To define network port of Syslog Monitor

Usage: Enter a valid network port number

Monitor Raw Data File Size:

Description: To define raw data file size in kilo bytes (kB), the percentage (%) to remove data in FIFO manner when file overflows its limit, and the time interval in minutes (min) to check the file size.

Usage: Enter values in ‘kB,%,min’ format

Monitor Alarm File Size:

Description: To define alarm file size in kilo bytes (kB), the percentage (%) to remove data in FIFO manner when file overflows its limit, and the time interval in minutes (min) to check the file size.

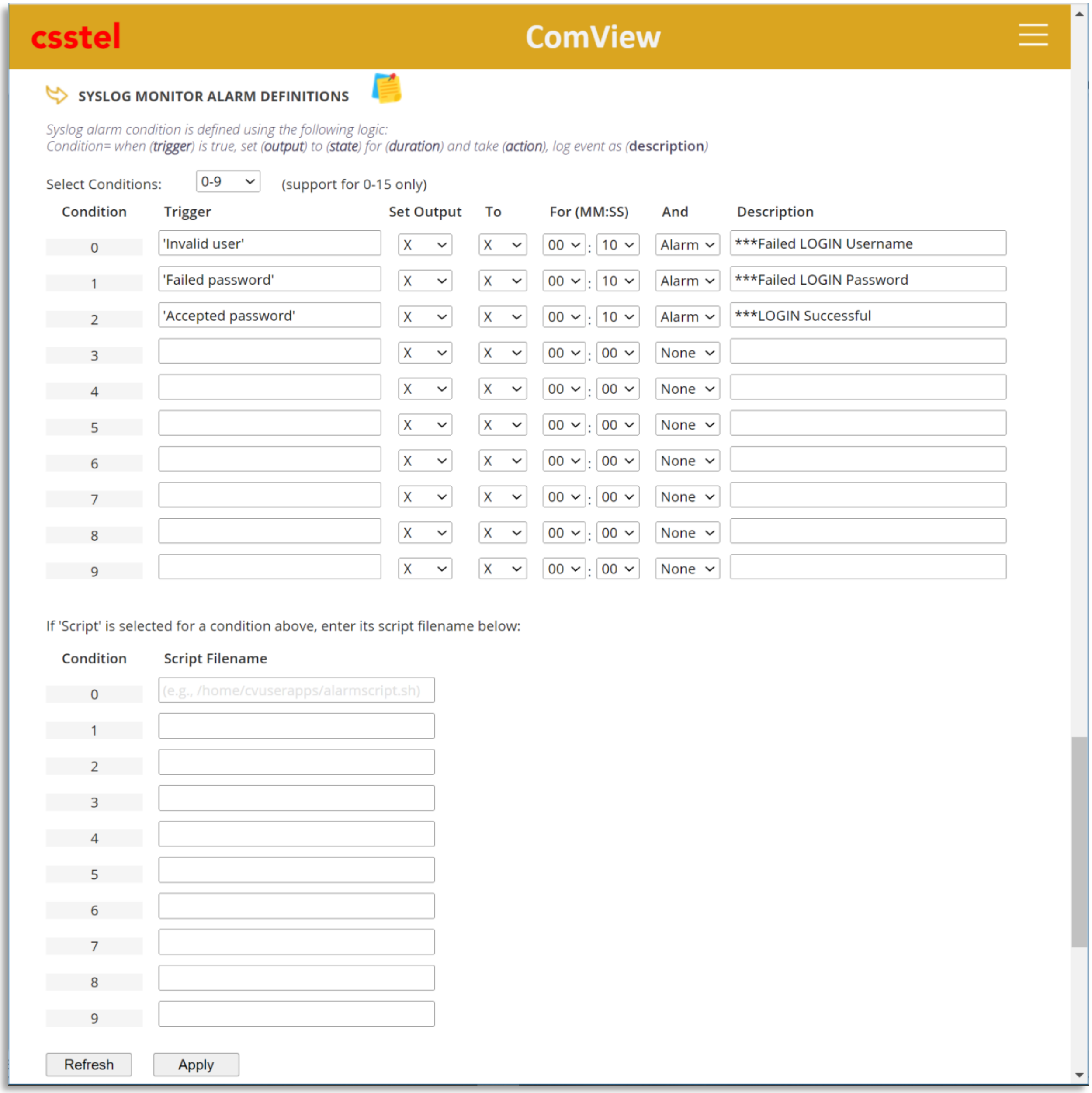
Usage: Enter values in ‘kB,%,min’ format

Syslog Data Logging Enable:

Description: To enable or disable Syslog data logging in external USB drive

Usage: Select [Yes,No]

The second section of Syslog Monitor configuration lets you define alarm conditions by setting values in the fields accordingly, as shown in the screenshot below:



SYSLOG MONITOR ALARM DEFINITIONS

Syslog alarm condition is defined using the following logic:
*Condition= when (**trigger**) is true, set (**output**) to (**state**) for (**duration**) and take (**action**), log event as (**description**)*

Select Conditions: 0-9 (support for 0-15 only)

Condition	Trigger	Set Output	To	For (MM:SS)	And	Description
0	'Invalid user'	X	X	00 : 10	Alarm	***Failed LOGIN Username
1	'Failed password'	X	X	00 : 10	Alarm	***Failed LOGIN Password
2	'Accepted password'	X	X	00 : 10	Alarm	***LOGIN Successful
3		X	X	00 : 00	None	
4		X	X	00 : 00	None	
5		X	X	00 : 00	None	
6		X	X	00 : 00	None	
7		X	X	00 : 00	None	
8		X	X	00 : 00	None	
9		X	X	00 : 00	None	

If 'Script' is selected for a condition above, enter its script filename below:

Condition	Script Filename
0	(e.g., /home/cvuserapps/alarmscript.sh)
1	
2	
3	
4	
5	
6	
7	
8	
9	

Syslog Monitor app implements the following expression to help users define an alarm condition more clearly and easily:

> Condition= when (**trigger**) is true, set (**output**) to (**state**) for (**duration**) and take (**action**), log event as (**description**)

The expression above is then mapped to columnar format for user entries as shown in the screenshot. These columns have the following syntax and usage:

Trigger: regular expression in single quotes (we entered 'Invalid user', 'Failed password', and 'Accepted password' strings for condition 0, 1, and 2 respectively)

Set Output: Dropdown list [X,0..5] to select output number to set when an alarm is detected:

- X: for 'not used' (i.e., no output selection)
- 0..5: to use Output[0..5]

To: Dropdown list [X, On, Off] to select the state to set the selected output port (i.e., output relay) on detected alarm

- X (uppercase): for no change for current state
- On: to set output to On; i.e., output relay is energized
- Off: to set output to Off; i.e., output relay is deenergized

For (MM:SS): in MM:SS format for Min:Sec, the time duration to set output state:

- Valid time range is [00:00 - 59:59]
- Value 00:00 sets the output state without resetting it

And: Dropdown list [None, Alarm, Script] to select action to take on alarm condition:

- None: no action to take
- Alarm: send alarm notifications via methods enabled
- Script: full pathname to executable user-specific bash script file (e.g., '/home/cvuserapps/myscript.sh') to execute immediately on alarm condition

Description: user description of alarm condition (we entered '***Failed LOGIN Username', '***Failed LOGIN Password', and '***LOGIN Successful'):

- Up to 30 characters (including space)
- Comma ',' not allowed (since comma is used as data field separator)

In the screenshot above, we completed setting up 3 alarm conditions with 'Invalid user', 'Failed password', and 'Accepted password' as alarm signatures to monitor syslog events for alarms. We also set action to 'Alarm' for alarm notifications with alarm description as '***Failed LOGIN Username', '***Failed LOGIN Password', and '***LOGIN Successful'.

Setup Verification

To verify our setup, we need to confirm that syslog messages sent to ComView are received and logged in its raw data file, alarms are logged in alarm files, and notifications are received on alarm.

To generate syslog messages, you attempt to login your network device with incorrect username, incorrect password, and correct username/password. With proper setup, ComView should receive log messages and generate alarms.

In this application note, we attempt to login a device at an IP address of 192.168.0.131. Since we configure Syslog Monitor app mode to 'Both' (Raw and Alarm) previously, Syslog Monitor captures log messages and stores them in its raw data file, alarms are logged in alarm files, and notifications are delivered on alarm.

Raw Data File '/tmp/cvdata/cvSyslogAppRaw.txt'

```
…
Nov  4 14:21:51 192.168.0.131 184 <45>1 2022-11-04T14:21:51+00:00 Tester131 syslog-ng 738 -
[meta sequenceId="3"] Syslog connection established; fd='27',
server='AF_INET(192.168.0.113:514)', local='AF_INET(0.0.0.0:0)'
Nov  4 14:22:09 192.168.0.131 169 <85>1 2022-11-04T14:22:08+00:00 Tester131 sshd 2540 - -
pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser=
rhost=192.168.0.9  user=ubuntu
Nov  4 14:22:11 192.168.0.131 116 <38>1 2022-11-04T14:22:10+00:00 Tester131 sshd 2540 - -
Failed password for ubuntu from 192.168.0.9 port 64636 ssh2
Nov  4 14:22:24 192.168.0.131 116 <38>1 2022-11-04T14:22:23+00:00 Tester131 sshd 2540 - -
Failed password for ubuntu from 192.168.0.9 port 64636 ssh2
Nov  4 14:22:36 192.168.0.131 103 <38>1 2022-11-04T14:22:35+00:00 Tester131 sshd 2546 - -
Invalid user guest from 192.168.0.9 port 64650
Nov  4 14:22:38 192.168.0.131 102 <85>1 2022-11-04T14:22:37+00:00 Tester131 sshd 2546 - -
pam_unix(sshd:auth): check pass; user unknown
Nov  4 14:22:38 192.168.0.131 156 <85>1 2022-11-04T14:22:37+00:00 Tester131 sshd 2546 - -
pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser=
rhost=192.168.0.9
Nov  4 14:22:40 192.168.0.131 128 <38>1 2022-11-04T14:22:39+00:00 Tester131 sshd 2546 - -
Failed password for invalid user guest from 192.168.0.9 port 64650 ssh2
Nov  4 14:23:54 192.168.0.131 120 <34>1 2022-11-04T14:23:53+00:00 Tester131 sshd 2540 - -
fatal: Timeout before authentication for 192.168.0.9 port 64636
Nov  4 14:24:29 192.168.0.131 120 <34>1 2022-11-04T14:24:28+00:00 Tester131 sshd 2546 - -
fatal: Timeout before authentication for 192.168.0.9 port 64650
…
```

NOTES:
1). Above are raw syslog messages as received
2). Text highlighted to show signatures that we look for as alarm conditions

Alarm File '/tmp/cvdata/cvSyslogAppAlarm.txt'

```
…
20221104,142211,ethernet,SYSLOG-NG,'Failed password',192.168.0.131,***Failed LOGIN Password
Nov  4 14:22:11 192.168.0.131 116 <38>1 2022-11-04T14:22:10+00:00 Tester131 sshd 2540 - -
Failed password for ubuntu from 192.168.0.9 port 64636 ssh2

20221104,142224,ethernet,SYSLOG-NG,'Failed password',192.168.0.131,***Failed LOGIN Password
Nov  4 14:22:24 192.168.0.131 116 <38>1 2022-11-04T14:22:23+00:00 Tester131 sshd 2540 - -
Failed password for ubuntu from 192.168.0.9 port 64636 ssh2

20221104,142236,ethernet,SYSLOG-NG,'Invalid user',192.168.0.131,***Failed LOGIN Username
Nov  4 14:22:36 192.168.0.131 103 <38>1 2022-11-04T14:22:35+00:00 Tester131 sshd 2546 - -
Invalid user guest from 192.168.0.9 port 64650

20221104,142240,ethernet,SYSLOG-NG,'Failed password',192.168.0.131,***Failed LOGIN Password
Nov  4 14:22:40 192.168.0.131 128 <38>1 2022-11-04T14:22:39+00:00 Tester131 sshd 2546 - -
Failed password for invalid user guest from 192.168.0.9 port 64650 ssh2
…
```

NOTES:

1). Above are alarm records that Syslog Monitor app generated on alarm conditions
2). Text highlighted to show signatures detected and the description of alarm as we defined

System Alarm File '/tmp/cvdata/cvAlarms.txt'

ComView logs alarms from all alarm sources in one consolidated alarm file. For each alarm record it logs in this file, ComView also sends alarm notifications via delivery methods that users defined.

The following shows the alarm records from Syslog Monitor logged in the consolidated alarm file:

```
…
20221104,142211,ethernet,SYSLOG-NG,'Failed password',192.168.0.131,***Failed LOGIN Password
20221104,142224,ethernet,SYSLOG-NG,'Failed password',192.168.0.131,***Failed LOGIN Password
20221104,142236,ethernet,SYSLOG-NG,'Invalid user',192.168.0.131,***Failed LOGIN Username
20221104,142240,ethernet,SYSLOG-NG,'Failed password',192.168.0.131,***Failed LOGIN Password
…
```

ComView device notifies users of alarm conditions as listed in the consolidated alarm file, while the Syslog Monitor alarm file provides more details on the notified alarms.

Summary

This application note illustrates how ComView Syslog Monitor app can be configured to detect alarm conditions in syslog messages sent by network devices with Syslog-NG support. Syslog Monitor app can also be set up as syslog collector to log incoming logs from these network devices.

About CSSTEL

CSSTEL is a privately held developer and manufacturer of ComView hardware and software solutions for secure, remote infrastructure site management since 1997 with installations in over 30 countries around the world.

We offer ComView solutions that are scalable and customizable to monitor and manage virtually the entire spectrum of remote site infrastructure and site conditions.

We help telecom service providers, carriers, financial institutions, healthcare providers, government agencies, utilities, and other public and private sector organizations maintain constant visibility and control over their remote site infrastructure.

IMPORTANT:

- CSSTEL Inc. assumes no responsibility for errors or omissions, or for damages resulting from the use of information contained in this document or from the use of programs and source code that accompany it. In no event shall CSSTEL Inc. be liable for any loss of profit, or any other commercial damage caused or alleged to have been caused directly or indirectly.

- No parts of this work may be reproduced in any form or by any means - graphic, electronic, or mechanical, including photocopying, recording, taping, or information storage and retrieval systems - without the written permission of CSSTEL Inc.

- Products that are referred to in this document may be either trademarks and/or registered trademarks of the respective owners. CSSTEL Inc. makes no claim to these trademarks.

- All rights reserved.

Revision History

Revision	Date	Description
1.00	2023-01-08	Initial release

*** End of document ***