Table of Contents

Syslog-ng install

NetYCE uses the public domain **Syslog-NG** package to provide SYSLOG services. The RedHat and CentOS distribution comes with the default **rsyslogd** that cannot provide the required services for the NCCM and Compliance functions.

Syslog-NG is needed for remote syslog signalling and to receive Syslog events from devices. This article describes the installation of Syslog-NG for RedHat/CentOS 6.x and 7.x in separate sections.

RHEL 6 (CentOS 6)

The required packages are not available by default through `yum`, so there are 2 choices: install using EPEL repo or install all packages using .rpm files both ways are documented:

option-1: YUM install

First install EPEL repo:

```
sudo yum --enablerepo=extras install epel-release
```

This installs the package:

```
epel-release-6-8.noarch
```

Then install syslog-ng and its dbi:

```
sudo yum install syslog-ng syslog-ng-libdbi
```

Sample session:

```
Dependencies Resolved

================================================================================
====
 Package                 Arch          Version                 Repository
Size
================================================================================
====
Installing:
 syslog-ng               x86_64        3.2.5-4.el6             epel
441 k
 syslog-ng-libdbi        x86_64        3.2.5-4.el6             epel
31 k
Installing for dependencies:
```

```
 eventlog                x86_64        0.2.13-1.el6           epel
17 k
 libdbi                  x86_64        0.8.3-4.el6            base
39 k
 libnet                  x86_64        1.1.6-7.el6            epel
58 k
```

This installs the packages:

```
eventlog-0.2.13-1.el6.x86_64.rpm
libdbi-0.8.3-4.el6.x86_64.rpm
libnet-1.1.6-7.el6.x86_64.rpm
syslog-ng-3.2.5-4.el6.x86_64.rpm
syslog-ng-libdbi-3.2.5-4.el6.x86_64.rpm
```

option-2: Manual install

NOTE: CentOS 6.x is no longer supported by 'yum' or most download locations. Try http://vault.centos.org/6.10 or download this .tgz file with the rpm files listed below:

syslog-ng-el6.tgz

Download the “rpm” packages for `syslog-ng` and its dependencies for RHEL6.

https://dl.fedoraproject.org/pub/epel/6/x86_64/Packages/e/eventlog-0.2.13-1.el6.x86_64.rpm

https://dl.fedoraproject.org/pub/epel/6/x86_64/Packages/l/libnet-1.1.6-7.el6.x86_64.rpm

https://dl.fedoraproject.org/pub/epel/6/x86_64/Packages/s/syslog-ng-3.2.5-4.el6.x86_64.rpm

https://dl.fedoraproject.org/pub/archive/fedora/linux/core/6/x86_64/os/Fedora/RPMS/libdbi-0.8.1-2.1.x86_64.rpm

https://dl.fedoraproject.org/pub/epel/6/x86_64/Packages/s/syslog-ng-libdbi-3.2.5-4.el6.x86_64.rpm

After downloading, copy these files to `/var/tmp/syslog-ng`

Install the packages:

```
cd /var/tmp/syslog-ng

(in case you downloaded the .tgz file unpack this with 'cd /var/tmp/syslog-ng; gtar xvzf syslog-ng-el6.tgz')

sudo rpm -Uvh *.rpm
```

Remove rsyslog

The RHEL6 systems come preinstalled with `rsyslog`. It must be disabled, but removing it is preferred:

```
sudo yum erase rsyslog
```

This removes the package:

```
rsyslog-5.8.10-12.el6.x86_64
```

Configuration

Syslog-ng config

```
sudo vim /etc/syslog-ng/syslog-ng.conf
```

The Syslog-ng configuration file needs some modifications. It is best replaced with the file below if there are no customer specific changes. This config adds the 'net' facility for udp and tcp, adds dns resolving using fqdn and re-timestamping. The network syslog messages are directed to the **`/var/opt/yce/logs/syslog-ng.log`** file.

It is this log-file that will be monitored by the `yce_events` daemon to signal NCCM configuration changes.

syslog-ng.conf

```
@version:3.2

# syslog-ng configuration file for NetYCE.
#
# This should behave pretty much like the original syslog on RedHat.
# See syslog-ng(8) and syslog-ng.conf(5) for more information.
#

options {
        flush_lines (0);
        time_reopen (10);
        log_fifo_size (1000);
        chain_hostnames (off);
        use_dns (yes);
        use_fqdn (yes);
        create_dirs (no);
        keep_hostname (yes);
        keep-timestamp (no);
};
```

```
source net {
        tcp();
        udp();
};

source s_sys {
        file ("/proc/kmsg" program_override("kernel: "));
        unix-stream ("/dev/log");
        internal();
        # udp(ip(0.0.0.0) port(514));
};

destination d_logs {
        file(
                "/var/opt/yce/logs/syslog-ng.log"
                owner("yce")
                group("nms")
                perm(0644)
        );
};
destination d_cons { file("/dev/console"); };
destination d_mesg { file("/var/log/messages"); };
destination d_auth { file("/var/log/secure"); };
destination d_mail { file("/var/log/maillog" flush_lines(10)); };
destination d_spol { file("/var/log/spooler"); };
destination d_boot { file("/var/log/boot.log"); };
destination d_cron { file("/var/log/cron"); };
destination d_kern { file("/var/log/kern"); };
destination d_mlal { usertty("*"); };

filter f_kernel     { facility(kern); };
filter f_default    {
        level(info..emerg) and
        not (facility(mail)
        or facility(authpriv)
        or facility(cron));
};
filter f_auth       { facility(authpriv); };
filter f_mail       { facility(mail); };
filter f_emergency  { level(emerg); };
filter f_news       {
        facility(uucp) or
        (facility(news)
        and level(crit..emerg));
};

filter f_boot   { facility(local7); };
filter f_cron   { facility(cron); };

log { source(net); destination(d_logs); };
```

```
log { source(s_sys); filter(f_kernel); destination(d_kern); };
#log { source(s_sys); filter(f_kernel); destination(d_cons); };
log { source(s_sys); filter(f_default); destination(d_mesg); };
log { source(s_sys); filter(f_auth); destination(d_auth); };
log { source(s_sys); filter(f_mail); destination(d_mail); };
log { source(s_sys); filter(f_emergency); destination(d_mlal); };
log { source(s_sys); filter(f_news); destination(d_spol); };
log { source(s_sys); filter(f_boot); destination(d_boot); };
log { source(s_sys); filter(f_cron); destination(d_cron); };

# end
```

Syslog-ng startup

Enable the syslog-ng as startup daemon and start the service

```
sudo chkconfig --add syslog-ng
sudo chkconfig --level 2345 syslog-ng on
sudo chkconfig --list syslog-ng
sudo service syslog-ng start
```

RHEL7 (CentOS 7)

The required packages are not available by default through yum, so there are 2 choices: install using EPEL repo or install all packages using .rpm files both ways are documented:

option-1: YUM install

> Note: On CentOS7 **yum** did not seem to need EPEL-repo on the systems we worked with. But as this might be due to an earlier install where “extras: ftp.tudelft.nl” was added. To be safe, we included this step anyway.

Add EPEL support for yum

```
   sudo yum --enablerepo=extras install epel-release
```

Then, install syslog-ng and its dbi using:

```
   sudo yum install syslog-ng syslog-ng-libdbi
```

Sample session:

```
yce@release7 /opt/yce/system
$ sudo yum install syslog-ng syslog-ng-libdbi
```

```
Loaded plugins: fastestmirror
Loading mirror speeds from cached hostfile
epel/x86_64/metalink
|  29 kB  00:00:00
Could not retrieve mirrorlist
https://mirrors.iuscommunity.org/mirrorlist?repo=ius-centos7&arch=x86_64&pro
tocol=http error was
14: curl#6 - "Could not resolve host: mirrors.iuscommunity.org; Unknown
error"
 * base: centos.mirror.triple-it.nl
 * epel: mirror.hostnet.nl
 * extras: ftp.tudelft.nl
 * updates: mirror.vimexx.nl
base
| 3.6 kB  00:00:00
extras
| 2.9 kB  00:00:00
ius
| 1.3 kB  00:00:00
mariadb
| 2.9 kB  00:00:00
mysecureshell
|  951 B  00:00:00
updates
| 2.9 kB  00:00:00
Resolving Dependencies
--> Running transaction check
---> Package syslog-ng.x86_64 0:3.5.6-3.el7 will be installed
--> Processing Dependency: ivykis >= 0.36.1 for package: syslog-
ng-3.5.6-3.el7.x86_64
--> Processing Dependency: libivykis.so.0(IVYKIS_0.29)(64bit) for package:
syslog-ng-3.5.6-3.el7.x86_64
--> Processing Dependency: libivykis.so.0(IVYKIS_0.30)(64bit) for package:
syslog-ng-3.5.6-3.el7.x86_64
--> Processing Dependency: libevtlog.so.0()(64bit) for package: syslog-
ng-3.5.6-3.el7.x86_64
--> Processing Dependency: libivykis.so.0()(64bit) for package: syslog-
ng-3.5.6-3.el7.x86_64
--> Processing Dependency: libnet.so.1()(64bit) for package: syslog-
ng-3.5.6-3.el7.x86_64
---> Package syslog-ng-libdbi.x86_64 0:3.5.6-3.el7 will be installed
--> Processing Dependency: libdbi.so.0()(64bit) for package: syslog-ng-
libdbi-3.5.6-3.el7.x86_64
--> Running transaction check
---> Package eventlog.x86_64 0:0.2.13-4.el7 will be installed
---> Package ivykis.x86_64 0:0.36.2-2.el7 will be installed
---> Package libdbi.x86_64 0:0.8.4-6.el7 will be installed
---> Package libnet.x86_64 0:1.1.6-7.el7 will be installed
--> Finished Dependency Resolution
```

```
Dependencies Resolved

================================================================================
=================================
 Package                          Arch                  Version
Repository           Size
================================================================================
=================================
Installing:
 syslog-ng                        x86_64                3.5.6-3.el7
epel                453 k
 syslog-ng-libdbi                 x86_64                3.5.6-3.el7
epel                 43 k
Installing for dependencies:
 eventlog                         x86_64                0.2.13-4.el7
epel                 19 k
 ivykis                           x86_64                0.36.2-2.el7
epel                 35 k
 libdbi                           x86_64                0.8.4-6.el7
base                 42 k
 libnet                           x86_64                1.1.6-7.el7
base                 59 k

Transaction Summary
================================================================================
=================================
Install  2 Packages (+4 Dependent packages)

Total download size: 651 k
Installed size: 2.0 M
Is this ok [y/d/N]:
```

Acknowledge and installation completes automatically.

option-2: Manual install

When no yum repository is available, a manual install is needed. The `syslog-ng` installation has some dependencies that requires that several packages must be downloaded, transferred to the server and installed as a group using `rpm`.

Package name	**Package version**	**Package rpm-file**
syslog-ng.x86_64	0:3.5.6-3.el7	syslog-ng-3.5.6-3.el7.x86_64.rpm
syslog-ng-libdbi.x86_64	0:3.5.6-3.el7	syslog-ng-libdbi-3.5.6-3.el7.x86_64.rpm
eventlog.x86_64	0:0.2.13-4.el7	eventlog-0.2.13-4.el7.x86_64.rpm
ivykis.x86_64	0:0.36.2-2.el7	ivykis-0.36.2-2.el7.x86_64.rpm
libdbi.x86_64	0:0.8.4-6.el7	libdbi-0.8.4-6.el7.x86_64.rpm
libnet.x86_64	0:1.1.6-7.el7	libnet-1.1.6-7.el7.x86_64.rpm

Download these packages from `centos.pkgs.org`:

https://centos.pkgs.org/7/centos-x86_64/libnet-1.1.6-7.el7.x86_64.rpm.html

https://centos.pkgs.org/7/centos-x86_64/libdbi-0.8.4-6.el7.x86_64.rpm.html

https://centos.pkgs.org/7/epel-x86_64/ivykis-0.36.2-2.el7.x86_64.rpm.html

https://centos.pkgs.org/7/epel-x86_64/eventlog-0.2.13-4.el7.x86_64.rpm.html

https://centos.pkgs.org/7/epel-x86_64/syslog-ng-3.5.6-3.el7.x86_64.rpm.html

https://centos.pkgs.org/7/epel-x86_64/syslog-ng-libdbi-3.5.6-3.el7.x86_64.rpm.html

Or download this .tgz file with all aforementioned rpm files:

syslog-ng-el7.tgz

Copy the downloaded rpm files to `/var/tmp/syslog-ng`.

Install the packages:

```
cd /var/tmp/syslog-ng

(in case you downloaded the .tgz file unpack this with cd /var/tmp/syslog-
ng; gtar xvzf syslog-ng-el7.tgz)

sudo rpm -Uvh *.rpm
```

Remove rsyslog

RHEL7 comes preinstalled with `rsyslog` which must be disabled. Removing the package is preferred.

```
sudo yum erase rsyslog
```

This removes the package:

```
rsyslog.x86_64 0:8.24.0-34.el7
```

Configuration

Syslog-ng config

```
sudo vim /etc/syslog-ng/syslog-ng.conf
```

The Syslog-ng configuration file needs some modifications. It is best replaced with the file below if there are no customer specific changes. This config adds the 'net' facility for udp and tcp, adds dns

resolving using fqdn and re-timestamping. The network syslog messages are directed to the **`/var/opt/yce/logs/syslog-ng.log`** file.

It is this log-file that will be monitored by the `yce_events` daemon to signal NCCM configuration changes.

syslog-ng.conf

```
@version:3.5
@include "scl.conf"

# RHEL7 syslog-ng configuration file for NetYCE.
#
# This should behave pretty much like the original syslog on RedHat.
# See syslog-ng(8) and syslog-ng.conf(5) for more information.
#
# Note: it also sources additional configuration files (*.conf)
#       located in /etc/syslog-ng/conf.d/

options {
    flush_lines (0);
    time_reopen (10);
    log_fifo_size (1000);
    chain_hostnames (off);
    use_dns (yes);
    use_fqdn (yes);
    create_dirs (no);
    keep_hostname (yes);
    keep-timestamp (no);
};

source net {
    tcp();
    udp();
};

source s_sys {
    system();
    internal();
    # udp(ip(0.0.0.0) port(514));
};

destination d_logs {
    file(
        "/var/opt/yce/logs/syslog-ng.log"
        owner("yce")
        group("nms")
        perm(0644)
    );
};
```

```
destination d_cons { file("/dev/console"); };
destination d_mesg { file("/var/log/messages"); };
destination d_auth { file("/var/log/secure"); };
destination d_mail { file("/var/log/maillog" flush_lines(10)); };
destination d_spol { file("/var/log/spooler"); };
destination d_boot { file("/var/log/boot.log"); };
destination d_cron { file("/var/log/cron"); };
destination d_kern { file("/var/log/kern"); };
destination d_mlal { usertty("*"); };

filter f_kernel     { facility(kern); };
filter f_default    {
    level(info..emerg) and
    not (facility(mail)
    or facility(authpriv)
    or facility(cron));
};
filter f_auth       { facility(authpriv); };
filter f_mail       { facility(mail); };
filter f_emergency  { level(emerg); };
filter f_news       {
    facility(uucp) or
    (facility(news)
    and level(crit..emerg));
};
filter f_boot   { facility(local7); };
filter f_cron   { facility(cron); };

log { source(net); destination(d_logs); };
log { source(s_sys); filter(f_kernel); destination(d_kern); };
#log { source(s_sys); filter(f_kernel); destination(d_cons); };
log { source(s_sys); filter(f_default); destination(d_mesg); };
log { source(s_sys); filter(f_auth); destination(d_auth); };
log { source(s_sys); filter(f_mail); destination(d_mail); };
log { source(s_sys); filter(f_emergency); destination(d_mlal); };
log { source(s_sys); filter(f_news); destination(d_spol); };
log { source(s_sys); filter(f_boot); destination(d_boot); };
log { source(s_sys); filter(f_cron); destination(d_cron); };


# Source additional configuration files (.conf extension only)
@include "/etc/syslog-ng/conf.d/*.conf"

# vim:ft=syslog-ng:ai:si:ts=4:sw=4:et:
```

Syslog-ng startup

Start the syslog-ng service

```
systemctl start syslog-ng

ps -ef | grep syslog
```

And enable to start at boot time too

```
systemctl enable syslog-ng
```

Yce_events configuration

After receiving a syslog message the syslog daemon (`syslog-ng`) will append it to the log file `/var/opt/yce/logs/syslog-ng.log`. It is another daemon, `yce_events`, that will monitor the messages in this log and try to match it against the various patterns in its configuration file. The matching messages can trigger an NCCM configuration fetch and subsequent compliance check.

To prevent continuous NCCM updates, the setup of each pattern uses a window of 10 minutes for each unique nodename or ip-address before retrieving the updated configuration. Some vendors will issue syslog messages for each command line changing the configuration, others may only signal once after a completed commit. For consistency reasons, it is recommended to keep the 'fetch-after-signal' delay a universal 10 minutes. But is desired, the window of 600 can be adjusted per message pattern to suit the environment.

The yce_event daemon is also responsible for resolving nodenames from the traditionally used ip-address and performs the required deduplication of messages when multiple message sources are used.

The **`yce_events`** configuration file is `/opt/yce/etc/`**`yce_events.conf`**. The configuration file lists the log-message patterns that signal a configuration change for the various NetYCE vendor modules. The initial distributed version of this configuration file can be found in `/opt/yce/`**`system`**`/yce_events.conf`. It is automatically copied to `/opt/yce/`**`etc`** when the configuration file cannot be found there.

Changes can be made to the “etc” version of the configuration file to suit the environment. If the syslog messages are not received directly from the devices but are forwarded using a different syslog receiver, the format of the messages are likely to have changed, requiring modified matching patterns in the configuration file.

As these message formats are different per syslog-receiver, NetYCE will gladly collect and provide patterns for the various syslog receivers. A “Kiwi” syslog-receiver file is listed underneath the vanilla yce_events.conf.

The file below reflects the current distribution configuration:

yce_events.conf

```
#
# (c) NetYCE, 2019
#
# yce_events configuration to detect configuration changes
```

```
# from network devices syslog messages
#
#
#------------------------------------------------------------
# Program options
#------------------------------------------------------------
#
type=StartupOptions
detach=yes
user=yce
group=nms
pid=/var/opt/yce/jobs/yce_events.pid
input=/var/opt/yce/logs/syslog-ng.log
log=/var/opt/yce/logs/yce_events.log
#
#
#------------------------------------------------------------
# Vendor Patterns
#------------------------------------------------------------
#
# Juniper
#
type=SingleWithSuppress
ptype=RegExp
pattern=.*\s(.*)\smgd\[\d+\]:\sUI_COMMIT_PROGRESS:(.*)commit\scomplete
desc=config save for $1
action=event config_changed_for_$1
window=600
#
# F5 BIGIP (still in development mode)
#
# Sample output for a config change:
# Jul 29 16:12:40 f5.netyce.org debug mcpd[4487]: Setting the master
key from memory.
# Jul 29 16:12:40 f5.netyce.org debug mcpd[4487]: save_master_key(7)
called
# Jul 29 16:12:40 f5.netyce.org debug mcpd[4487]: Saving the new
version of Master key file.
# Jul 29 16:12:40 f5.netyce.org debug mcpd[4487]: Wrote the new version
of Master key file.
# Jul 29 16:12:40 f5.netyce.org debug mcpd[4487]: Wrote the new version
of Recovery key file.
# Jul 29 16:12:40 f5.netyce.org debug mcpd[4487]: notify_master_key:
notification sent.
# Jul 29 16:12:41 f5.netyce.org notice tmsh[10999]: 01420002:5: AUDIT -
pid=10999 user=root folder=/Common module=(tmos)# status=[Command OK]
cmd_data=save /sys config
#
type=SingleWithSuppress
ptype=RegExp
```

```
pattern=[\w]{3} [\d]{1,2} [\S]{8} (\S*) notice [\w]+\[\d+\]: .* AUDIT -
.* status=\[Command OK\] cmd_data=save .* config
desc=config save for $1
action=event config_changed_for_$1
window=600
#
# HP_C7 normal save or save main
#
type=SingleWithSuppress
ptype=RegExp
pattern=[a-zA-
Z]{3}\s{1,2}\d{1,2}\s\d{2}:\d{2}:\d{2}\s(.*)\s%%10SHELL\/6\/SHELL_CMD_C
ONFIRM:\sConfirm\soption\sof\scommand\ssave\s
desc=config save for $1
action=event config_changed_for_$1
window=600
#
# HP_C7 normal save main force or save force
#
type=SingleWithSuppress
ptype=RegExp
pattern=[a-zA-
Z]{3}\s\d{1,2}\s\d{2}:\d{2}:\d{2}\s(.*)\s%%10SHELL\/6\/SHELL_CMD:\s.*Co
mmand\sis\ssave\s
desc=config save for $1
action=event config_changed_for_$1
window=600
#
# Arista_EOS
#
type=SingleWithSuppress
ptype=RegExp
pattern=[a-zA-
Z]{3}\s\d{1,2}\s\d{2}:\d{2}:\d{2}\s(.*)\sConfigAgent:\s%SYS-5-
CONFIG_STARTUP:\sStartup\sconfig\ssaved
desc=config save for $1
action=event config_changed_for_$1
window=600
#
# Cisco_Nexus
#
type=SingleWithSuppress
ptype=RegExp
pattern=[a-zA-
Z]{3}\s\d{1,2}\s\d{2}:\d{2}:\d{2}\s((\d{1,3})\.(\d{1,3})\.(\d{1,3})\.(\
d{1,3}))\s:\s\d{4}\s[a-zA-Z]{3}\s\d{1,2}\s\d{2}:\d{2}:\d{2}\s[A-
Z]{3}:\s%VSHD-5-VSHD_SYSLOG_CONFIG_I:\sConfigured\sfrom
desc=config save for $1
action=event config_changed_for_$1
window=600
#
```

```
# Cisco_IOS
#
type=SingleWithSuppress
ptype=RegExp
pattern=[a-zA-
Z]{3}\s+\d{1,2}\s\d{2}:\d{2}:\d{2}\s((\d{1,3})\.(\d{1,3})\.(\d{1,3})\.(
\d{1,3}))\s\d+:\s+\*[a-zA-
Z]{3}\s+\d{1,2}\s\d{2}:\d{2}:\d{2}(:|.\d{3}:)\s%SYS-5-
CONFIG_I:\sConfigured
desc=config save for $1
action=event config_changed_for_$1
window=600
#
# HP_C5 normal save, save main, save main force or save force
#
type=SingleWithSuppress
ptype=RegExp
pattern=[a-zA-
Z]{3}\s\d{1,2}\s\d{2}:\d{2}:\d{2}\s(.*)\s%%10CFM/5/CFM_SAVECONFIG_SUCCE
SSFULLY\(l\):\sConfiguration\sis\ssaved\ssuccessfully
desc=config save for $1
action=event config_changed_for_$1
window=600
#
# Avaya_ERS save
#
type=SingleWithSuppress
ptype=RegExp
pattern=[a-zA-
Z]{3}\s\d{1,2}\s\d{1,2}:\d{1,2}:\d{1,2}\s(\d{1,3})\.(\d{1,3})\.(\d{1,3}
)\.(\d{1,3})\s\d{2}:\d{2}:\d{2}:\d{2}\s(.*)\s:Trap:\s\sbsnConfiguration
SavedToNvram
desc=config save for $1
action=event config_changed_for_$1
window=600
#
# CI_6 save configuration
#
type=SingleWithSuppress
ptype=RegExp
pattern=[a-zA-
Z]{3}\s\d{1,2}\s\d{1,2}:\d{1,2}:\d{1,2}\s((\d{1,3})\.(\d{1,3})\.(\d{1,3
})\.(\d{1,3}))\s\[[a-
z]{5}\]\s((\d{1,3})\.(\d{1,3})\.(\d{1,3})\.(\d{1,3}))\s([0-9A-Fa-
f]{2}[:-]){5}([0-9A-Fa-f]{2})\s\d{4}\sCONFIG-5-CONFIG_SAVE:
desc=config save for $1
action=event config_changed_for_$1
window=600
#
#-------------------------------------------------------------
```

```
# External worker script
#------------------------------------------------------------
#
#type=SingleWithScript
#ptype=RegExp
#pattern=config_changed_for_(\S+)
#script=/opt/yce/bin/config_change.pl -l -d 2 -n $1
#desc=$0
#action=write - normal save OR save main node $1 matches.
#
#------------------------------------------------------------
# Internal worker script
#------------------------------------------------------------
#
type=SingleWithSub
ptype=RegExp
pattern=config_changed_for_(\S+)
sub=yce_nccm
arg=$1
desc=$0
action=write - normal save OR save main node $1 matches.
```

Yce_events.conf version for Kiwi:

yce_events.conf

```
#
# (c) NetYCE, 2020
#
# yce_events configuration to detect configuration changes
# from network devices syslog messages
#
#
#------------------------------------------------------------
# Program options
#------------------------------------------------------------
#
type=StartupOptions
detach=yes
user=yce
group=nms
pid=/var/opt/yce/jobs/yce_events.pid
input=/var/opt/yce/logs/syslog-ng.log
log=/var/opt/yce/logs/yce_events.log
#
#
#------------------------------------------------------------
# Vendor Patterns
#------------------------------------------------------------
#
```

```
# Juniper
#
type=SingleWithSuppress
ptype=RegExp
pattern=.*\s(.*)\smgd\[\d+\]:\sUI_COMMIT_PROGRESS:(.*)commit\scomplete
desc=config save for $1
action=event config_changed_for_$1
window=600
#
# F5 BIGIP (still in development mode)
#
# Sample output for a config change:
# Jul 29 16:12:40 f5.netyce.org debug mcpd[4487]: Setting the master
key from memory.
# Jul 29 16:12:40 f5.netyce.org debug mcpd[4487]: save_master_key(7)
called
# Jul 29 16:12:40 f5.netyce.org debug mcpd[4487]: Saving the new
version of Master key file.
# Jul 29 16:12:40 f5.netyce.org debug mcpd[4487]: Wrote the new version
of Master key file.
# Jul 29 16:12:40 f5.netyce.org debug mcpd[4487]: Wrote the new version
of Recovery key file.
# Jul 29 16:12:40 f5.netyce.org debug mcpd[4487]: notify_master_key:
notification sent.
# Jul 29 16:12:41 f5.netyce.org notice tmsh[10999]: 01420002:5: AUDIT -
pid=10999 user=root folder=/Common module=(tmos)# status=[Command OK]
cmd_data=save /sys config
#
type=SingleWithSuppress
ptype=RegExp
pattern=[\w]{3} [\d]{1,2} [\S]{8} (\S*) notice [\w]+\[\d+\]: .* AUDIT -
.* status=\[Command OK\] cmd_data=save .* config
desc=config save for $1
action=event config_changed_for_$1
window=600


#
# HP_C7 normal save or save main
#
#type=SingleWithSuppress
#ptype=RegExp
#pattern=[a-zA-
Z]{3}\s+\d{1,2}\s\d{2}:\d{2}:\d{2}\s.*\sOriginal\sAddress=(\d{1,3}\.\d{
1,3}\.\d{1,3}\.\d{1,3})\s[a-zA-
z]{3}\s\d{1,2}\s\d{2}:\d{2}:\d{2}\s\d+.*%%10CFGMAN/5/CFGMAN_CFGCHANGED
#desc=config save for $1
#action=event config_changed_for_$1
#window=600
#
```

```
# HP_C7 normal save main force or save force
#
type=SingleWithSuppress
ptype=RegExp
pattern=[a-zA-
Z]{3}\s\d{1,2}\s\d{2}:\d{2}:\d{2}\s(.*)\s%%10SHELL\/6\/SHELL_CMD:\s.*Co
mmand\sis\ssave\s
desc=config save for $1
action=event config_changed_for_$1
window=600
#
# Arista_EOS
#
type=SingleWithSuppress
ptype=RegExp
pattern=[a-zA-
Z]{3}\s\d{1,2}\s\d{2}:\d{2}:\d{2}\s(.*)\sConfigAgent:\s%SYS-5-
CONFIG_STARTUP:\sStartup\sconfig\ssaved
desc=config save for $1
action=event config_changed_for_$1
window=600
#
# Cisco_Nexus
#
type=SingleWithSuppress
ptype=RegExp
pattern=[a-zA-
Z]{3}\s+\d{1,2}\s\d{2}:\d{2}:\d{2}\s.*\sOriginal\sAddress[\s|=](\d{1,3}
\.\d{1,3}\.\d{1,3}\.\d{1,3})\s*:.*:\s*\%VSHD-5-
VSHD_SYSLOG_CONFIG_I:\sConfigured\sfrom
desc=config save for $1
action=event config_changed_for_$1
window=600
#
# Cisco_IOS
#
type=SingleWithSuppress
ptype=RegExp
pattern=[a-zA-
Z]{3}\s+\d{1,2}\s\d{2}:\d{2}:\d{2}\s.*\sOriginal\sAddress[\s|=](\d{1,3}
\.\d{1,3}\.\d{1,3}\.\d{1,3})\s\d+:.*%SYS-5-CONFIG_I:\sConfigured
desc=config save for $1
action=event config_changed_for_$1
window=600
#
# Cisco_XR
#
type=SingleWithSuppress
ptype=RegExp
pattern=[a-zA-
Z]{3}\s+\d{1,2}\s\d{2}:\d{2}:\d{2}\s.*\sOriginal\sAddress=(\d{1,3}\.\d{
```

```
1,3}\.\d{1,3}\.\d{1,3})\s[a-zA-
z]{3}\s+\d{1,2}\s\d{2}:\d{2}:\d{2}.\d{3}\s[A-
Z]{3}:\s+\d+:\sRP\/\d\/RSP\d\/CPU\d:[a-zA-
Z]{3}\s+\d{1,2}\s\d{2}:\d{2}:\d{2}.\d{3}\s[A-
Z]{3}:\sconfig\[\d+\]:\s%MGBL-SYS-5-CONFIG_I\s:\sConfigured
desc=config save for $1
action=event config_changed_for_$1
window=600

#
# HP_C5 normal save, save main, save main force or save force
#
type=SingleWithSuppress
ptype=RegExp
pattern=[a-zA-
Z]{3}\s+\d{1,2}\s\d{2}:\d{2}:\d{2}\s.*\sOriginal\sAddress=(\d{1,3}\.\d{
1,3}\.\d{1,3}\.\d{1,3})\s[a-zA-
z]{3}\s+\d{1,2}\s\d{2}:\d{2}:\d{2}\s\d+.*%%10CFGMAN/5/CFGMAN_CFGCHANGED
desc=config save for $1
action=event config_changed_for_$1
window=600
#
# HP_C5 different timestamp
#
type=SingleWithSuppress
ptype=RegExp
pattern=[a-zA-
Z]{3}\s+\d{1,2}\s\d{2}:\d{2}:\d{2}\s.*\sOriginal\sAddress=(\d{1,3}\.\d{
1,3}\.\d{1,3}\.\d{1,3})\s\d{4}-\d{2}-
\d{2}T\d{2}:\d{2}:\d{2}.*\s%%10CFGMAN/5/CFGMAN_CFGCHANGED
desc=config save for $1
action=event config_changed_for_$1
window=600
#
#
# Avaya_ERS save
#
type=SingleWithSuppress
ptype=RegExp
pattern=[a-zA-
Z]{3}\s\d{1,2}\s\d{1,2}:\d{1,2}:\d{1,2}\s(\d{1,3})\.(\d{1,3})\.(\d{1,3}
)\.(\d{1,3})\s\d{2}:\d{2}:\d{2}:\d{2}\s(.*)\s:Trap:\s\sbsnConfiguration
SavedToNvram
desc=config save for $1
action=event config_changed_for_$1
window=600
#
# CI_6 save configuration
#
type=SingleWithSuppress
```

```
ptype=RegExp
pattern=[a-zA-
Z]{3}\s\d{1,2}\s\d{1,2}:\d{1,2}:\d{1,2}\s((\d{1,3})\.(\d{1,3})\.(\d{1,3
})\.(\d{1,3}))\s\[[a-
z]{5}\]\s((\d{1,3})\.(\d{1,3})\.(\d{1,3})\.(\d{1,3}))\s([0-9A-Fa-
f]{2}[:-]){5}([0-9A-Fa-f]{2})\s\d{4}\sCONFIG-5-CONFIG_SAVE:
desc=config save for $1
action=event config_changed_for_$1
window=600
#
#-------------------------------------------------------------
# External worker script
#-------------------------------------------------------------
#
#type=SingleWithScript
#ptype=RegExp
#pattern=config_changed_for_(\S+)
#script=/opt/yce/bin/config_change.pl -l -d 2 -n $1
#desc=$0
#action=write - normal save OR save main node $1 matches.
#
#-------------------------------------------------------------
# Internal worker script
#-------------------------------------------------------------
#
type=SingleWithSub
ptype=RegExp
pattern=config_changed_for_(\S+)
sub=yce_nccm
arg=$1
desc=$0
action=write - normal save OR save main node $1 matches.
```

The NCCM matching patterns used above are verified. NetYCE collected other patterns that are supposedly usable for the same purpose but have not been verified, not are known to which vendor they belong.

These patterns are:

```
Startexecuting:set
Startexecuting:saveconfig
(?:PIX|ASA)-5-611103
cli.*USER.*COMMAND
AUDIT-.*modify
AUDIT-user\S+.*modify
SYS-6-CFG_CHG
SMETELNETfrom
SYS-5-CONFIG_I
CSCOacs
AAA-5-AAA_AUTH_ADMIN_USER:aaa.(.*)[\t]for[\t]admin[\t]user[\t]'(.*)'
```

```
SYSTEM_RESET
Leavingconfigurationmode
AUDIT-user\S+.*_delete
,set,
(?:PIX|ASA|FWSM)-5-111005
HWCM
(?:PIX|ASA)-5-199001
AUDIT-.*delete
SYS-5-CONFIG
command:sy.*
FWSM-6-605005
MANAGERMode
OSAPI-5-CLEAN_TASK:\s*osapi_task.c:(?:.*)cleaning\s*up\s*exited\s*task
Commandissy.*
Configurationchangedby
apache:.*POST
,delete,
daemonsys_message:installed
(?:PIX|ASA)-5-111005
Acceptedpasswordfor
,edit
SYSLOG_CONFIG
,commit,
```

syslog messages from different vendors

Vendor	Message
JunOS	Feb 19 15:23:06 <NODE-NAME> mgd[5053]: UI_COMMIT_COMPLETED: commit complete
Cisco Nexus	Feb 19 15:46:57 192.168.178.21 : 2020 Feb 19 14:46:59 UTC: %VSHD-5-VSHD_SYSLOG_CONFIG_I: Configured from vty by NetYCE on 192.168.178.25@pts/0
Cisco IOS	Feb 19 16:04:19 192.168.178.66 19: *Mar 1 00:03:44: %SYS-5-CONFIG_I: Configured from console by admin on vty0 (192.168.178.25)
Cisco XR	Feb 19 16:32:31 192.168.178.67 35: RP/0/0/CPU0:Feb 19 15:32:32.232 : config[65828]: %MGBL-CONFIG-6-DB_COMMIT : Configuration committed by user 'admin'. Use 'show configuration commit changes 1000000035' to view the changes.
Cisco XE	Feb 19 17:26:01 192.168.178.57 54: *Feb 19 16:26:02.806: %SYS-5-CONFIG_I: Configured from console by admin on vty0 (192.168.178.25)
BIGIP F5	Feb 19 17:37:39 <FQDN> notice tmsh[8828]: 01420002:5: AUDIT - pid=8828 user=root folder=/Common module=(tmos)# status=[Command OK] cmd_data=save /sys config
HP C5	Feb 21 16:38:52 TE–RN01001 10SHELL/6/SHELL_CMD(l): -Task=vt0-IPAddr=192.168.178.25-User=admin; Command is save | | HP C7 | Feb 19 17:48:55 <NODE-NAME> 10SHELL/6/SHELL_CMD_CONFIRM: Confirm option of command save is yes.
Arista EOS	Feb 19 17:56:48 <NODE-NAME> ConfigAgent: %SYS-5-CONFIG_I: Configured from console by admin on vty3 (192.168.178.25)
Aruba	Feb 20 11:52:41 <NODE-NAME> «NODE-NAME> 192.168.178.169> cli[5770]: USER:admin@192.168.178.25 NODE:“/mm/mynode” COMMAND:<write memory> – command executed successfully

Vendor	Message
HP C5	Feb 21 16:39:05 <NODE-NAME> %%10SHELL/6/SHELL_CMD(l): -Task=vt0-IPAddr=192.168.178.25-User=admin; Command is save force

Remarks

syslog-ng

- syslog-ng is not managed by yce_psmon. It must be started as system facility

- DNS (reverse) resolver is not used in syslog-ng. Since NetYCE requires only a small subset of syslog events to catch configuration changes, this task befalls yce_events

- The syslog logfile, `/var/opt/yce/logs/syslog-ng.log`, potentially receives way too much info if ALL syslog messages are sent or forwarded to NetYCE. There is currently no filtering on incoming syslog messages.

- log rotation '/var/opt/yce/logs/syslog-ng.log' to be added to log_maint.pl. Will require the daemon to be restarted.

Testlog.pl

To perform functional and performance tests on the syslog-ng / yce_events setup the following perl script could be used as a base for generating spoofed syslog messages.

testlog.pl

```
#!/opt/ycelib/perl/bin/perl
#
#

use lib "/opt/yce/YCE";
use Common;
use File::Basename;
use Time::HiRes qw(gettimeofday tv_interval sleep);
use Time::Local;
use Data::Dumper;
$Data::Dumper::Indent = 1;

# use strict;
# use warnings;

use Sys::Syslog qw(:standard :extended :macros);

$loghost = '172.17.10.28';
# $proto = 'udp';
$proto = 'tcp';
```

```
# $proto = 'inet';

$ident = '172.17.10.21';
$logopt = "ndelay,pid";
$facility = "net";

$rc = setlogsock($proto, $loghost);
print "setlogsock -> $rc\n";

$rc = openlog($ident, $logopt, $facility);
print "openlog -> $rc\n";

$level = 'info';
$message = "A $facility.$level syslog message to $loghost from $ident
using $proto from $0:$$";


print "sending: $message\n";
$rc = syslog("$level", $message);
print "syslog -> $rc\n";

1;
```