Integrating Syslog-NG and LMS 3.1

White Paper

Syslog-NG Integration with LMS 3.1

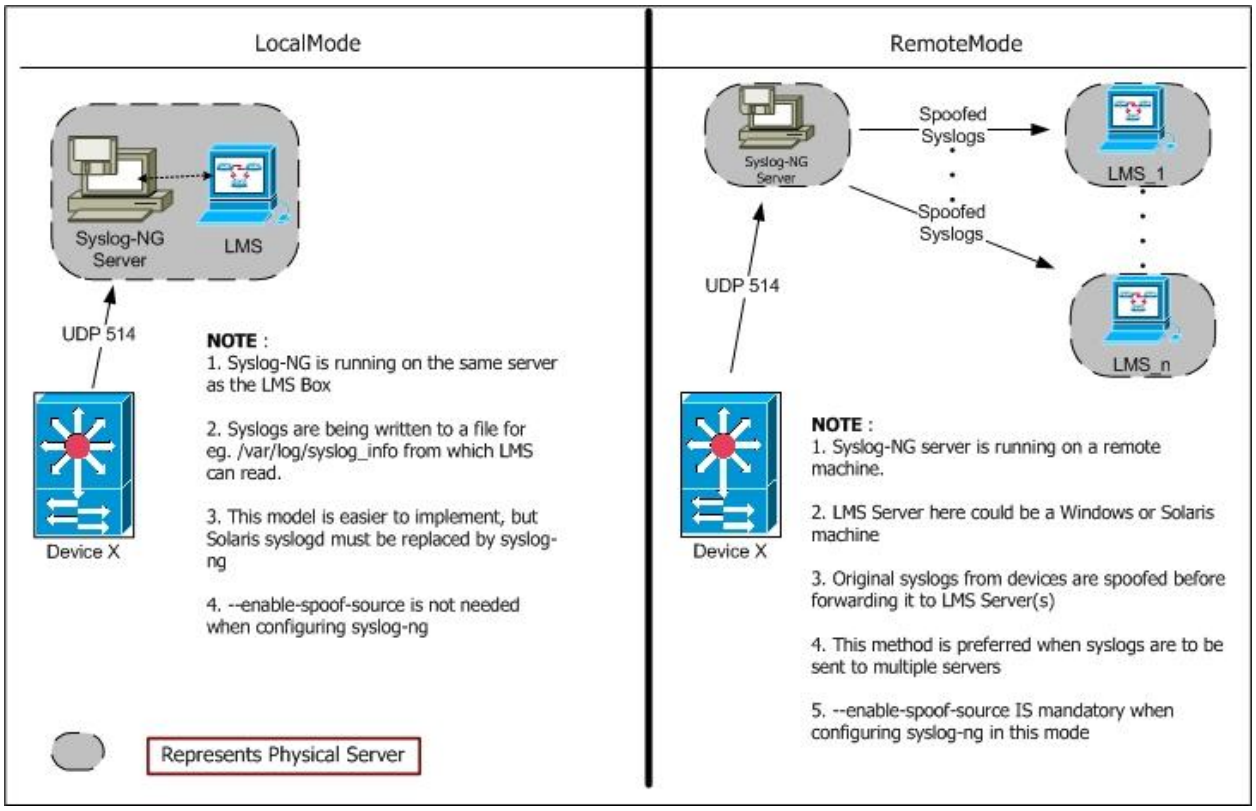
1 Introduction

1.1 What is Syslog-NG?

As per their website, Syslog-NG embodies the next generation of logging systems, and is the first truly flexible and scalable system logging application. Syslog-NG is an open source implementation of the Syslog protocol for UNIX and UNIX-like systems. It extends the original *syslogd* model with content-based filtering, rich filtering capabilities, and flexible configuration options and adds important features to syslog, like using TCP for transport.

1.2 How does it work?

1.2.1 The overview of how syslogs-ng works is shown in the figure below.



Devices can send syslogs to the Syslog-NG server. Syslog-NG can be configured to spoof the syslogs and filter/forward them as original syslogs to Ciscoworks LMS servers as needed. When we say spoof, we mean changing the IP Address of the original sender (in this case, device originating the syslogs).

1.2.2 Disadvantages of Spoofing:

1. UDP failure to deliver may be reported back to the device instead of Syslog-NG
2. Won't work if there is a firewall rule between the Syslog-NG and the LMS Server. Will work only if the traffic from Syslog-NG is allowed.

2 Matrix of Syslog-NG and LMS 3.1

	Mode of Operation	Type of syslogd running on LMS Server	Destination Method
1	LocalMode	Syslog-NG **(Win OR Sol10)**	Write to File
2	RemoteMode	Solaris 10 "syslogd"	Forwarded spoofed syslogs
3	RemoteMode	Solaris 10 "syslog-ng"	Forwarded spoofed syslogs
4	RemoteMode	Windows	Forwarded spoofed syslogs

3 How to Install Syslog-NG?

3.1 Syslog-NG Install

3.1.1 Compiling Syslog-NG from source:

Install the entire Syslog-NG prerequisites from the URL below:
http://www.balabit.com/network-security/syslog-ng/opensource-logging-system/compiling/

Once that is done, you will need to compile syslogs-ng as follows.

3.1.2 Configure Options:

Must configure Syslog-NG with *"--enable-spoof-source*" in order to enable spoof_source feature (which is disabled by default).

```
./configure --enable-spoof-source
```

3.1.3 Make & Install:

Once you successfully configure, you can proceed to the installation as follows:

```
$ make
```

And then

```
$ make install
```

If you run into any issues during the install, you can refer to the syslogs-ng forum at:
https://lists.balabit.hu/mailman/listinfo/syslog-ng
OR
you can refer to their knowledge base at:
http://www.balabit.com/support/knowledge_base/kbsearch.bbq?kw=product_syslog-ng

NOTE: Cisco TAC will not able to provide installation/compile support for Syslog-NG though.

3.2 Sample Reference Configuration file:

Below is a sample Config file that could be used as is to get a quick jump start. Users will need to modify the IP Address/Ports and other such local information as per their environment.

```
############################################################
# First, set some global options.
options {
        use_fqdn(no);
        use_dns(no);
        long_hostnames(off);
        sync(0);
};
# Then, set some global sources.
source src {
        udp(ip("0.0.0.0") port(514));
};
# Then, set some global destinations.
destination Remote_LMS_SyslogNG {
        udp("192.168.141.43" port(514) spoof_source(yes));
        udp("192.168.141.44" port(514) spoof_source(yes));
        udp("192.168.141.45" port(514) spoof_source(yes));
        udp("192.168.141.46" port(514) spoof_source(yes));
                                        };
destination Local_LMS_SyslogNG {
        file("/var/log/syslogs_info"
                template("$DATE $HOST $MSG\n")
             );
                                        };
# Now log it
log {
        source(src);
# if using Remote LMS, turn On the following:
#        destination(Remote_LMS_SyslogNG);
# if running SyslogNG Locally on LMS, turn On the following:
#        destination(Local_LMS_SyslogNG);
      };
############################################################
```

3.3 SyslogAnalyzer process must be restarted on LMS Server

3.3.1 Restarting from the GUI

Navigate to Common Services > *Admin* > *Processes* > Look for *SyslogAnalyzer* > Check that row and click on "*Stop*". Once that process is stopped, check the same row (if Unchecked) and click on "*Start*".

3.3.2 Restarting from CLI

Windows:

Stop SyslogAnalyzer

```
C:\Program Files\CSCOpx\bin\pdterm SyslogCollector SyslogAnalyzer
```

Start SyslogAnalyzer

```
C:\Program Files\CSCOpx\bin\pdexec SyslogCollector SyslogAnalyzer
```

Verify SyslogAnalyzer

```
C:\Program Files\CSCOpx\bin\pdshow SyslogCollector SyslogAnalyzer
```

Solaris:

Stop SyslogAnalyzer

```
# /opt/CSCOpx/bin/pdterm SyslogCollector SyslogAnalyzer
```

Start SyslogAnalyzer

```
# /opt/CSCOpx/bin/pdexec SyslogCollector SyslogAnalyzer
```

Verify SyslogAnalyzer

```
# /opt/CSCOpx/bin/pdshow SyslogCollector SyslogAnalyzer
```

3.3.3 PACE Solution and Syslog-NG

In this situation, we need to point the syslogs from Syslog-NG server to NCM machine in the PACE solution if LMS/NCM are installed on different machines.

4 Reference

- http://www.balabit.com/network-security/syslog-ng/opensource-logging-system/
- http://www.balabit.com/network-security/syslog-ng/opensource-logging-system/compiling/
- http://en.wikipedia.org/wiki/Syslog-ng
- http://www.campin.net/syslog-ng/faq.html
- https://lists.balabit.hu/mailman/listinfo/syslog-ng
- http://www.balabit.com/support/knowledge_base/kbsearch.bbq?kw=product_syslog-ng