Syslog Cheat Sheet (v1.2)

https://www.aplura.com/cheatsheets

Common Variables

Syslog-ng		Rsyslog	
Sending host	$HOST	Sending host	fromhost
Sending host IP	$SOURCEIP	Sending host IP	fromhost-ip
Priority text	$PRIORITY	Priority text	pri-text
Facility text	$FACILITY	Facility text	syslogfacility-text
Tag	$TAGS	Tag	syslogtag
Program name	$PROGRAM	Program name	programname
Time received	${R_DATE}	Time received	timegenerated
Message time	${DATE}	Message time	timereported

syslog-ng parameters | rsyslog properties

Setup Listeners

```
source s_remote_all {
        udp ( ip("0.0.0.0") port(514) );
        tcp ( ip("0.0.0.0") port(514) ); };
source s_firewall {
        udp ( ip("0.0.0.0") port(1514) );
        tcp ( ip("0.0.0.0") port(1514) ); };
```

```
input(type="imudp" port="514" ruleset="f_remote_all")
input(type="imtcp" port="514" ruleset="f_remote_all")
input(type="imudp" port="1514" ruleset="f_firewall")
input(type="imtcp" port="1514" ruleset="f_firewall")
```

Filters (*Optional*)

```
# Syslog-ng filters are defined separately
and used within the log statement
filter f_firewall_range {
netmask (192.168.100.0/255.255.255.0); };
```

Syslog-ng Filter Options

gray, italicized items are optional

```
# Rsyslog filters go within the Output ruleset
if ($fromhost-ip startswith '192.168.100.')
then { action(type="omfile"
DynaFile="d_firewall_log")
}
```

Rsyslog Expressions
Rsyslog Control Structures

Organize Directories by Host

```
destination d_catch_all { file("/var/log/remote_syslog/
catch_all/$HOST/$YEAR-$MONTH-$DAY.log"); };

destination d_firewall_log { file("/var/log/
remote_syslog/firewall/$HOST/$YEAR-$MONTH-$DAY.log"); };
```

```
template(name="d_catch_all" type="string" string="/var/
log/remote_syslog/catch_all/%FROMHOST%/%$YEAR%-%$MONTH%-%
$DAY%.log")
template(name="d_firewall_log" type="string" string="/var/
log/remote_syslog/firewall/%FROMHOST%/%$YEAR%-%$MONTH%-%
$DAY%.log")
```

Set Output

```
log { source(s_remote_all);
      destination(d_catch_all); };
log { source(s_firewall); filter(f_firewall_range);
      destination(d_firewall_log); };
```

```
ruleset(name="f_remote_all") {
    action(type="omfile" DynaFile="d_catch_all") }
ruleset(name="f_firewall") {
    action(type="omfile" DynaFile="d_firewall_log") }
```

Performance Tuning

```
options {
        log_fifo_size (10000);
        time_reap(20);
        flush_lines(10000);
        flush_timeout(1000); };
```

syslog_ng_tuning

```
main_queue(
queue.size="1000000"   # Size of Queue
queue.debatchsize="1000"  # process messages in batches
queue.workerthreads="2"  # 2 threads for the queue
)
```

rsyslog_tuning

Permissions

POSIX ACLs

`chmod g+s /var/log/remote_syslog/`	Set the SUID bit
`setfacl -R -d -m g:splunk:rx /var/log/remote_syslog/`	Set the default permissions
`setfacl -R -m g:splunk:rx /var/log/remote_syslog/`	Set the current permissions
`setfacl -R -x g:splunk:rx /var/log/remote_syslog/`	Remove POSIX permissions
`chmod g-s /var/log/remote_syslog/`	Remove SUID bit

SELINUX

`chcon system_u:object_r:var_log_t:s0 /var/log/remote_syslog/`	Set the selinux context
`restorecon -R -v /var/log/remote_syslog/`	Apply to existing files
`semanage port -a -t syslogd_port_t -p udp 1514`	Allow port

APLURA
Many Solutions, One Goal.

Common Syslog configurations

Syslog-ng

gray, italicized items are optional

```
@version:3.2
options {
        log_fifo_size (10000);
        time_reap(20);
        flush_lines(10000);
        flush_timeout(1000);
        create_dirs(yes); };
source s_remote_all {
        udp ( ip("0.0.0.0") port(514) );
        tcp ( ip("0.0.0.0") port(514) );
};
source s_firewall {
        udp ( ip("0.0.0.0") port(1514) );
        tcp ( ip("0.0.0.0") port(1514) );
};

filter f_firewall_range {
        netmask (192.168.100.0/255.255.255.0); };

destination d_catch_all {
        file("/var/log/remote_syslog/catch_all/$HOST/
$YEAR-$MONTH-$DAY.log");
};

destination d_firewall_log {
        file("/var/log/remote_syslog/firewall/$HOST/
$YEAR-$MONTH-$DAY.log");
};

log {
   source(s_remote_all);
   destination(d_catch_all); };
log {
   source(s_firewall); filter(f_firewall_range);
   destination(d_firewall_log); };
```

syslog-ng documentation

For a more commented version of this config:

syslog-ng config

Rsyslog

```
$PreserveFQDN on
$CreateDirs on
# Sources

main_queue(
queue.size="1000000"
queue.debatchsize="1000"
queue.workerthreads="2")

module(load="imtcp" MaxSessions="5000")
module(load="imudp")

input(type="imudp" port="514" ruleset="f_remote_all")
input(type="imtcp" port="514" ruleset="f_remote_all")
input(type="imudp" port="1514" ruleset="f_firewall")
input(type="imtcp" port="1514" ruleset="f_firewall")

# Destinations
template(name="d_catch_all" type="string" string="/var/
log/remote_syslog/catch_all/%FROMHOST%/%$YEAR%-%
$MONTH%-%$DAY%.log")
template(name="d_firewall_log" type="string" string="/
var/log/remote_syslog/firewall/%FROMHOST%/%$YEAR%-%
$MONTH%-%$DAY%.log")

ruleset(name="f_remote_all" queue.type="LinkedList"
queue.size="100000") {
if ($fromhost-ip startswith '192.168.100.') then {
   action(type="omfile" DynaFile="d_firewall_log")
   stop
}
# Lets setup the catch all logging
action(type="omfile" DynaFile="d_catch_all")
}
ruleset(name="f_firewall") {
action(type="omfile" DynaFile="d_firewall_log") }
```

rsyslog documentation

For a more commented version of this config:

rsyslog config

Check Syntax

```
syslog-ng --syntax-only
```

```
rsyslogd -N1 -f /etc/rsyslog.conf
```

OS Tuning

sysctl.conf

Paramater	Value	Description
fs.file-max	2097152	Increase file handles & inode cache
net.ipv4.tcp_max_syn_backlog	8192	Max syns without an ack
net.core.netdev_max_backlog	65536	Increase packet backlog queue
net.core.optmem_max	25165824	Max kernel memory buffer
net.ipv4.tcp_mem	65536 131072 262144	Buffer size range (TCP)
net.ipv4.udp_mem	65536 131072 262144	Buffer size range (UDP)
net.core.rmem_default	25165824	Socket receive buffer default
net.core.rmem_max	25165824	Max receive memory
net.ipv4.tcp_rmem	20480 12582912 25165824	Receive buffer size range (TCP)
net.ipv4.udp_rmem	20480 12582912 25165824	Receive buffer size range (UDP)

limits.conf

User	Type	Item	Value	Descrption
root	hard	nofile	65536	Set the file handle limit
root	soft	nofile	10240	Set the file handle limit
syslog	hard	nofile	65536	Set the file handle limit
syslog	hard	nofile	10240	Set the file handle limit