

 **ONE IDENTITY™**

Syslog-ng 101, part 6: Destinations and log path

Peter Czanik

Destination Definition

- Destinations contain one or more destination drivers where syslog-ng sends (stores) log messages:

```
destination <identifier> {  
    destination-driver(parameters);  
    destination-driver(parameters); ...  
};
```

- A simple file destination:

```
destination d_file {  
    file("/var/log/syslog");  
};
```

Destination drivers

- `file()`: writes to a file
- `pipe()`: writes to a named pipe
- `unix-stream()` and `unix-dgram()`: writes to a socket
- `network()`: sends legacy messages over the network
- `usertty()`: writes to a logged in user terminal
- `program()`: writes to a program's standard input
- `syslog()`: writes the RFC5424 syslog family standard
- `python()`: write your own code in Python
- `http()`: Elasticsearch, Slack, many cloud services
- Many more

Further elements

- Options: set global behavior of syslog-ng
- Macro: element of a parsed log message. They can be used for reconstructing messages.
- Template: user-defined expression for reformatting (restructuring) log messages (for example, adding timezone)
- Filter: expression for selecting (filtering) messages
- Parser: separates message into smaller parts by a separator. The result can be used as a name-value pair in templates.
- Rewrite: a sed-like tool that modifies a part of the message.

The log path

- Defines the route of the incoming log messages:

```
log {  
    source(s_id1);  
    destination(d_id1);  
};
```

- The log path can contain flags, filters and other objects:

```
log {  
    source(s_id1); source (s_id2);...  
    filter(f_id1); filter(f_id2);...  
    destination(d_id1); destination(d_id2);...  
    flags(flag1[,flag2...]);  
};
```

syslog-ng.conf: minimal

```
@version:3.38
```

```
source s_sys { system(); internal();};
```

```
destination d_mesg { file("/var/log/messages"); };
```

```
log { source(s_sys); destination(d_mesg); };
```

syslog-ng.conf: most typical components

```
@version:3.19
@include "scl.conf"

# this is a comment :)

options {flush_lines (0); keep_hostname (yes);};

source s_sys { system(); internal();};
destination d_mesg { file("/var/log/messages"); };
filter f_default { level(info..emerg) and not (facility(mail)); };

log { source(s_sys); filter(f_default); destination(d_mesg); };
```


Syntax check

- Using the `-s` option
- No output, no problem:

```
QDNDV8D3:~ # syslog-ng -s -f /etc/syslog-ng/first.conf
QDNDV8D3:~ #
```

- Well, there could be still typos...

 **ONE IDENTITY™**