

 **ONE IDENTITY™**

# Syslog-ng 101, part 4: Configuration and testing

Peter Czanik

# Configuring syslog-ng

- “Don't Panic”
- Simple and logical, even if it looks difficult at first
- Pipeline model:
  - Many different building blocks (sources, destinations, filters, parsers, etc.)
  - Connected into a pipeline using “log” statements

# **/etc/syslog-ng/syslog-ng.conf: getting started**

```
@version:3.38
```

```
@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); };
```

# SCL: syslog-ng configuration library

- A collection of configuration snippets
- Work like any syslog-ng driver
- Application Adapters (automatic message parsing)
- Credit-card number anonymization
- elasticsearch-http() destination
- and a lot more

# Starting syslog-ng

- By default starts in the background
- `systemctl [stop|start] syslog-ng`
- Important options:
  - `-s`: syntax check
  - `-F`: start in foreground
  - `-vde`: print debug messages on terminal
  - `-f path/to/config`: use alternate configuration

# Testing syslog-ng

- Test it in the foreground
  - Easier to see configuration problems
  - Easier to stop (^C)
- Tools:
  - logger: sends a single message
  - loggen: benchmarking, sending logs from files

# Testing steps

- Stop the running logging implementation
- Save the sample config on your host
- Start syslog-ng in the foreground using the saved config:
  - `syslog-ng -Fvde -f /path/to/config.conf`
- In another terminal:
  - `logger this is a test`
  - `tail /var/log/messages`



 **ONE IDENTITY™**