

 **ONE IDENTITY™**

# Syslog-ng 101, part 9: Filters

Peter Czanik

# Declaring filters

- Filters are expressions to select (filter) log messages
- For example, discard debug level messages or route authentication messages to SIEM
- Defined just like any other building block:

```
filter name { filterfunction(); };
```

```
filter f_default { level(info..emerg) and not (facility(mail)); };
```

# Common filter functions

- level: filters for the severity
- facility: filters for the facility
- host: filters hostname
- program: filters for the running program
- match: filters by regular expression
- netmask: filters by sender IP or subnet
- filter: uses a different filter

## Example

```
@version:3.38
```

```
@include "scl.conf"
```

```
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);  
};
```

# THE INLIST() FILTER

- Filtering based on white- or blacklisting
- Compares a single field with a list of values
- One value per line in text file
- Use cases
  - Poor man's SIEM: alerting based on spammer / C&C / etc. IP address lists
  - Filtering based on a list of application names

## If/else

- Conditional expressions in log path
- Makes it easier to use the results of filtering
- `if (filter()) { do this }; else { do that };`
- For example, use different parsers on different logs

# Example

```
@version:3.38
@include "scl.conf"

source s_sys { system(); internal(); };
destination d_mesg { file("/var/log/messages"); };
log { source(s_sys); destination(d_mesg); };

filter f_sudo {program("sudo")};

destination d_sudoall {
  file("/var/log/sudo.json"
  template("${format-json --scope nv_pairs --scope dot_nv_pairs --scope rfc5424}\n\n"));
};

log {
  source(s_sys);
  filter(f_sudo);
  if (match("workshop" value(".sudo.SUBJECT"))) {
    destination { file("/var/log/sudo_filtered"); };
  };
  destination(d_sudoall);
};
```



 **ONE IDENTITY™**