

 **ONE IDENTITY™**

# **Syslog-ng 101, part 8: Macros and templates**

Peter Czanik

# Macros

- Macros are variables defined by syslog-ng
  - As one syslog message arrives, syslog-ng parses it
  - Macros contain parsed message parts or converted formats
- Example syslog-ng macros:
  - \$FACILITY, \$PRIORITY
  - \$DATE, \$ISODATE, \$YEAR, \$MONTH, \$WEEK, \$DAY, \$HOUR, \$MINUTE etc.
- Name-value pairs:
  - variables defined by any syslog-ng parser or rule, like the CSV parser or a rewrite rule
  - often used interchangeably

# Templates

- Templates can be used to create standard message formats or filenames.
- A simple message formatting template and its usage:

```
template t_syslog {  
    template("$ISODATE $HOST $MSG\n");  
};  
destination d_syslog {  
    file("/var/log/syslog" template(t_syslog));  
};
```

# Templates

- A simple file path defined by template:

```
destination t_demo1 {  
    file("/var/log/$HOST/messages.log" create_dirs(yes));  
};
```

```
destination t_demo2 {  
    file("/var/log/$HOST_messages.log");  
};
```

# Log rotation

- Log rotation using syslog-ng macros:

```
destination d_messages {  
    file( "/var/log/$R_YEAR/$R_MONTH/$HOST_$R_DAY.log"  
create_dirs(yes));  
};
```

 **ONE IDENTITY™**